SÃ©curiser son environnement virtuel pour les PME
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 16/12/2010 14:00:00

Bien plus qu'un phÃ©nomÃ¨ne de mode, la virtualisation s'est imposÃ©e comme une technologie rÃ©volutionnaire et une tendance incontournable au sein des organisations. Pourtant, la ruÃ©e vers la virtualisation ne devrait pas dissimuler les problÃ¨mes de sÃ©curitÃ© qui se cachent derriÃ¨re elle. **Virtualisons!**

La virtualisation est aujourd'hui devenue un outil clef pour les entreprises, apportant de nombreux avantages tant dans le domaine informatique que dans le domaine du commerce et des affaires. Dans ses dÃ©buts, la technologie Ã©tait principalement utilisÃ©e pour consolider les serveurs et ressources informatiques dans un souci dâ□□Ã©conomie, de gain d'espace et d'Ã©nergie. Depuis, la virtualisation a trouvÃ© de nombreuses autres applications et modes d'utilisation. Les entreprises lâ□□utilisent par exemple pour accroÃ®tre leur flexibilitÃ© opÃ©rationnelle et informatique, pour amÃ©liorer la disponibilitÃ© et le dÃ©ploiement de leurs applications, pour rÃ©duire les risques de temps dâ□□arrÃªt et assurer une meilleure continuitÃ© des activitÃ©s, pour renforcer les contrÃ´les sur leur infrastructure, ou encore pour optimiser et simplifier la gestion des ressources et des activitÃ©s.

Au niveau du serveur, la virtualisation permet de dÃ©coupler les ressources physiques du systÃ¨me d'exploitation (OS) et des applications. Elle rompt le lien rigide qui existe entre le matÃ©riel et le logiciel, et permet de faire fonctionner plusieurs instances d'un systÃ¨me d'exploitation et plusieurs applications logicielles Ã partir dâ□□un seul et mÃªme ordinateur physique. En d'autres termes, la virtualisation permet dâ□□extraire et de calquer le systÃ¨me d'exploitation et les applications logicielles dans une machine virtuelle (MV). Cet ensemble virtuel - CPU, mÃ©moire et rÃ©seau, OS et applications - est transformÃ© alors en un fichier logiciel unique. Les machines virtuelles sont indÃ©pendantes des machines physiques et peuvent Ãªtre manipulÃ©es en toute simplicitÃ©, comme des fichiers, aussi facilement quâ□□un copier-coller.

Le moniteur MV, ou hyperviseur, permet d'accÃ©der Ã partir des ressources physiques aux multiples machines virtuelles ou â□□hÃ´tesâ□□. Les ressources matÃ©rielles sont rÃ©unies et allouÃ©es dynamiquement en fonction des besoins de chaque application, tandis que les machines virtuelles sont isolÃ©es les unes des autres et encapsulÃ©es (facile Ã stocker, dÃ©placer, etc.). Ceci permet de rÃ©aliser de nombreux Ã©conomies: gains de matÃ©riel, dâ□□Ã©nergie et dâ□□espace; consolidation du systÃ¨me et optimisation des infrastructures; rÃ©duction des coÃ»ts du personnel, rÃ©duction de la complexitÃ© globale, mise en Å□uvre et gestion simplifiÃ©e.

Pour mieux comprendre la virtualisation et son impact sur le monde informatique, il suffit de comparer la technique aux services bancaires Ã©lectroniques. Une fois lâ□□argent dÃ©posÃ© en espÃ¨ces dans le systÃ¨me, celui-ci est transformÃ© en monnaie Ã©lectronique et peut Ãªtre dÃ©placÃ© Ã travers le monde avec vitesse de l'Ã©clair, car il est virtuel ; il est information. En transformant les structures physiques en information (octets), la virtualisation apporte un nouveau niveau d'efficacitÃ© et de souplesse Ã l'environnement informatique. En particulier, elle permet de

provisionner et de gÃ©rer toute l'infrastructure informatique de maniÃ¨re plus rapide et plus agile.

RÃ©seaux virtuels et dÃ©fis sÃ©curitaires

Conquise par ses nombreux avantages Ã©conomiques et techniques, l'industrie informatique sâ□□est vue rapidement prise dâ□□assaut par la virtualisation. Pourtant, les environnements virtualitÃ©s comportent Ã©galement de nombreux risques sÃ©curitaires, contre lesquels les entreprises devraient Ãªtre mises en garde.

En effet, la virtualisation introduit une couche supplÃ©mentaire au sein de l'infrastructure informatique. Les logiciels de sÃ©curitÃ© traditionnels, conÃ§us pour les environnements physiques, manquent de visibilitÃ© sur cette nouvelle plateforme, ce qui crÃ©e des vulnÃ©rabilitÃ©s potentielles au sein du rÃ©seau et un manque de visibilitÃ© dans le trafic inter-MV. Les nouvelles machines virtuelles, installÃ©s automatiquement sur la plateforme (en particulier en cas de prolifÃ©ration des machines virtuelles ou â□□MV Sprawlâ□□), doivent Ãªtre protÃ©gÃ©es, systÃ©matiquement. De mÃªme, les machines virtuelles en cours de migration d'une plateforme physique Ã un autre -- en raison de l'expansion des infrastructures ou de dÃ©faillance matÃ©rielle -- doivent Ãªtre protÃ©gÃ©s et surveillÃ©s afin de ne pas interrompre le service lors de leur migration Ã chaud.

Outre ces menaces internes, les organisations doivent Ã©galement protÃ©ger leurs environnements virtuels contre les menaces externes. Les environnements virtuels peuvent en fait Ãªtre beaucoup plus dangereux que les environnements physiques, dans la mesure oÃ¹ les mÃªmes techniques d'attaque et les mÃªmes menaces qui existent dans le monde matÃ©riel prÃ©valent vraisemblablement aussi dans la plate-forme virtuelle, oÃ¹ les applications ne sont pas physiquement cloisonnÃ©es.

Cela signifie que si le serveur hÃ´te est attaquÃ© et que la couche virtuelle est compromise, l'ensemble des MVs prÃ©sentes sur lâ□□infrastructure virtuelle sera exposÃ© et toutes les applications et bases de donnÃ©es hÃ©bergÃ©es seront potentiellement compromises.

Les rÃ©seaux virtuels prÃ©sentent non seulement les mÃªmes dÃ©fis sÃ©curitaires que les rÃ©seaux physiques, mais ont aussi leurs enjeux propres. Pour assurer leur sÃ©curitÃ©, les organisations doivent mettre en place des solutions spÃ©cifiques et des technologies adÃ©quates afin de mieux contrÃ´ler leur rÃ©seau virtuel, de le protÃ©ger contre les menaces internes comme externes et dâ□□en assurer la bonne mise en conformitÃ©.

Comment protÃ©ger efficacement votre rÃ©seau virtuel

La solution idÃ©ale doit assurer aux machines virtuelles et applications le mÃªme niveau de sÃ©curitÃ© que sur les serveurs physiques:

â□¢ Tout d'abord il convient de sÃ©parer les machines virtuelles et de protÃ©ger le trafic inter-MV, en agissant au cÅ□ur mÃªme de la plate-forme de virtualisation, au niveau de lâ□□hyperviseur. Lâ□□intÃ©gration avec l'hyperviseur est capitale, car la protection doit Ãªtre dÃ©ployÃ©e non seulement au niveau de la machine virtuelle, mais commencer dÃ¨s l'hyperviseur lui-mÃªme.

â□¢ DeuxiÃ¨mement, la solution doit protÃ©ger contre les menaces extÃ©rieures, et donc Ãªtre dotÃ©e dâ□□un bon pare-feu et dâ□□un systÃ¨me de prÃ©vention des intrusions (IPS) efficace.

â¢ TroisiÃ¨mement, elle doit fournir une gestion unifiÃ©e pour l'environnement physique et pour l'environnement virtuel, afin de faciliter la gestion de la sÃ©curitÃ© pour les administrateurs.

â¢ Il est important que la solution assure toutes ces fonctions sans pour autant compromettre la flexibilitÃ© et l'extensibilitÃ© du systÃ¨me virtuel. En effet les protections sont lÃ avant tout pour permettre de dÃ©ployer et de profiter de la stratÃ©gie de virtualisation et non en attÃ©nuer les bÃ©nÃ©fices.

â¢ Enfin, la solution doit assurer une protection de systÃ¨me Ã tous les niveaux - pas seulement au niveau du rÃ©seau. Toutes les mesures de protection appliquÃ©es au trafic dans le monde physique doivent Ãªtre dÃ©ployÃ©es Ã©galement dans l'environnement virtualisÃ©.

Check Point Security Gateway Virtual Edition (VE), la nouvelle solution de sÃ©curisation des machines virtuelles de Check Point, offre toutes ces possibilitÃ©s. BasÃ©e sur lâArchitecture Software Bladeâ¢ de Check Point et certifiÃ©e par MVware, la solution offre aux applications virtuelles le mÃªme niveau supÃ©rieur de sÃ©curitÃ© quâaux applications situÃ©es sur des serveurs physiques. La solution protÃ¨ge les environnements virtualisÃ©s et les rÃ©seaux externes contre les menaces internes et externes en inspectant tout le trafic inter-MV au niveau de lâhyperviseur, et en sâappuyant sur des politiques de pare-feu granulaire et une fonctionnalitÃ© intÃ©grÃ©e de prÃ©vention des intrusions. Les machines virtuelles sont protÃ©gÃ©es Ã la fois contre les menaces externes et les unes contre les autres, Ã travers le spectre de protections UTM (Unified Threat Management), comprenant pare-feu intÃ©grÃ© et systÃ¨me IPS performant, VPN (Virtual Private Network), antivirus, anti-spam, filtrage d'URL et de la sÃ©curitÃ© Web.

Tout comme un boÃ®tier de sÃ©curitÃ© traditionnel couvre plusieurs systÃ¨mes sur un rÃ©seau, l'appliance virtuelle permet de sÃ©curiser de multiples machines virtuelles, tout bÃ©nÃ©ficiant de la stratÃ©gie de virtualisation. VE fonctionne directement Ã l'intÃ©rieur de la plateforme virtuelle et utilise la technologie MVsafe de MVware pour renforcer la sÃ©curitÃ© au sein de l'hyperviseur. Pour amÃ©liorer la sÃ©curitÃ© des rÃ©seaux, la solution permet de sÃ©parer les applications virtuelles les unes des autres. La protection de la machine virtuelle nâest pas interrompue durant la migration en temps rÃ©el des machines virtuelles d'un hÃ´te Ã lâautre, ni lorsque de nouvelles machines virtuelles sont ajoutÃ©es. Cela garantit une continuitÃ© de service, zÃ©ro temps dâarrÃªt, lorsque les machines virtuelles sont dÃ©placÃ©es d'un hÃ´te Ã l'autre pour maintenance ou allocation dynamique des ressources.

Check Point Security Gateway VE offre aussi une plateforme de gestion unique pour les environnements physiques et virtuels. Cette plateforme unifiÃ©e simplifie la gestion de la sÃ©curitÃ© et permet une nette sÃ©paration des fonctions entre administrateurs de la virtualisation et administrateurs de la sÃ©curitÃ©. La vÃ©rification et mise en conformitÃ© sont Ã©galement rendues plus faciles et plus rapides grÃ¢ce Ã un reporting adaptÃ© pour l'infrastructure virtuelle.

Conclusion

Comme toutes les technologies Ã©mergentes, la virtualisation amÃ¨ne de nouveaux risques pour les entreprises. Choisir une architecture de sÃ©curitÃ© adaptÃ©e Ã lâenvironnement virtuel, et bien se protÃ©ger contre les menaces internes et externes, est une nÃ©cessitÃ© pour les responsables informatiques, sâils veulent profiter pleinement de leur stratÃ©gie de virtualisation.

Pour plus d'informations

Â

[**Oded Gonda**, vice-prÃ©sident des produits de sÃ©curitÃ© rÃ©seau chez Check Point Software.]