

SĂ©curit   : SĂ©curiser le r  seau virtuel, un d  fi du Cloud-Computing

PostÃ© par : JPilo

Publié le : 16/4/2010 0:00:00

Stonesoft : 5 mÃ©thodes pour sÃ©curiser le rÃ©seau virtuel,Â le dÃ©fi le plus significatif du cloud computingÂ L'Ã©diteur finlandais dÃ©voile cinq mÃ©thodes pour rÃ©soudre les problÃ©mes de sÃ©curitÃ© dans le cloud

Stonesoft, fournisseur innovant de solutions intégrées de sécurité et de continuité de service, a identifié cinq faiblesses, pour les entreprises, démontrant la sécurité du cloud computing. Cette annonce vient renforcer la toute dernière communication émanant du Gartner qui explique que d'ici 2012, 60 % des serveurs virtualisés seront moins sécurisés que les serveurs physiques qu'ils sont censés remplacer (Source : Addressing the Most Common Security Risks in Data Center Virtualization Projects, Janvier 2010).

Actuellement, la plupart des entreprises d'exploient sur leur réseau des technologies de virtualisation sans impliquer les équipes réseau et de sécurité des systèmes dans les phases de planification. Il en résulte la chose suivante : la majorité des entreprises se contente donc de moderniser les réseaux virtuels, en y appliquant les politiques de sécurité réseaux physiques existantes. Ce manque de préparation et de perspective affaiblit considérablement la sécurité du réseau, cette dernière étant l'élément essentiel de la mise en place réussie du cloud computing au sein des très grandes entreprises.

Pour appuyer cette communication du Gartner, Stonesoft a identifi  cinq fa ons pour les  quipes informatiques de se pr munir des menaces et attaques survenant dans le cloud, tout en assurant la bonne mise en  uvre de leurs politiques



1. Regrouper les identités (Federated ID): le besoin pour les collaborateurs de se connecter à de multiples applications et services est inhérent à tout environnement de type cloud. La possibilité d'assurer l'authentification forte de l'utilisateur risquant d'aboutir aux entreprises, ceci représente donc un énorme danger en termes de sécurité. Pour réduire ce risque, les entreprises doivent mettre en place des technologies de Single Sign-On (SSO), similaires, par exemple, à celle de la StoneGate SSL VPN. Elles vont permettre aux utilisateurs d'accéder, via un login unique, à de multiples applications et services y compris ceux localisés en dehors de la société, dans le cloud public. Le SSO permettra aux entreprises d'harmoniser l'administration de la sécurité et d'assurer l'authentification forte même dans le cloud.

2. Assurer une connectivité permanente :

lorsque la plupart des données sensibles d'une entreprise sont stockées dans le cloud, la moindre panne réseau risque d'interrompre les opérations commerciales. Les services du cloud doivent être constamment accessibles, et ce même pendant les opérations de maintenance : des fonctionnalités de haute-disponibilité comme le clustering actif/actif, un serveur dynamique de répartition de charge, ainsi qu'un répartiteur de chargeur ISP doivent donc être mis en place au sein de l'infrastructure réseau. Il est préférable pour les entreprises de choisir des technologies d'intégration à l'infrastructure réseau, plutôt que d'investir dans des versions

autonomes de solutions ; le tout afin d assurer l efficacit , la facilit  d administration mais  galement de r duire les co ts.

3. Mettre en place une inspection multi-couches : de l augmentation du nombre d environnements cloud computing et de la multiplication de menaces toujours plus  volu es d coule le besoin de cr er une protection couche-par-couche, comprenant la protection p rim riale, la pr vention et la d tection d intrusions sur le r seau. Au lieu de mettre en place des firewalls de premi re g n ration visant   prot ger le cloud et son p rim tre, Stonesoft pr f re le d ploiement d appliances firewalls virtuelles de nouvelle g n ration (comme par exemple la StoneGate Virtual NextGen Firewall) qui int grent un firewall et un IPS pour une inspection en profondeur du trafic. Ainsi, les entreprises pourront analyser tous les types de trafic : de la navigation web, aux applications peer-to-peer en passant par le trafic web chiff  transitant dans le tunnel SSL. Des appliances IPS suppl mentaires devront aussi  tre install es afin de prot ger les r seaux des attaques internes qui menacent l acc s au cloud.

4. Exiger une administration centralis e : l erreur humaine reste toujours la menace la plus consid rable pesant   la fois sur les r seaux virtuels et physiques. A mesure que les entreprises d ploient des dispositifs r seaux suppl mentaires afin de s curiser leur r seau virtuel, le risque devient plus grand. En effet, la gestion des p riph riques, la surveillance et la configuration deviennent plus complexes et totalement d sorganis es. C est pour cette raison que Stonesoft recommande aux entreprises l utilisation d une seule console d administration pour g rer superviser et configurer l ensemble des dispositifs r seau, qu ils soient physiques, virtuels ou tiers.

5. Prot ger les postes de travail virtuels : de plus en plus d entreprises d cident de d ployer des postes de travail virtuels afin de b n ficier des avantages de cette nouvelle technologie notamment en ce qui concerne l administration et les co ts. Cependant, ces postes de travail sont tout autant, et si ce n est plus, vuln rables que leurs homologues physiques. Pour prot ger les postes de travail virtuels de fa on ad quate, les entreprises devront les isoler des autres segments du r seau et mettre en place des processus d inspection profonde pour pr venir les attaques internes et externes. Ces entreprises devront adopter une approche multi-niveaux de la s curit  en mettant notamment en place une technologie IPS qui emp chera les acc s internes non autoris s, prot gera les postes clients des serveurs malveillants et d livrera  galement des fonctionnalit s d acc s distants via l IPsec ou le SSL VPN qui prot ge contre les acc s externes non autoris s.

Stonesoft propose actuellement une gamme de solutions de s curit  virtuelle qui offre une protection avanc e du cloud. Cette offre est compos e de StoneGate Virtual NextGen Firewall, StoneGate Virtual IPS et StoneGate Virtual SSL VPN.

[Pour plus d informations](#)