Cloud Computing : Pour contrer au mieux les menaces informatiques.
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 13/1/2014 15:00:00

Zscaler, acteur majeur dans les services de sÃ©curitÃ© et de contrÃ´le du trafic Web des entreprises, publie un document prÃ©sentant ses prÃ©visions 2014 quant Ã la sÃ©curitÃ© dans le Cloud et met en avant **les Ã©cueils Ã Ã©viter pour contrer au mieux les menaces informatiques.**
2013 aura Ã©tÃ© marquÃ©e par d'importantes cyber-attaques et il est justifiÃ© de dire qu'aujourd'hui les anti-virus classiques ne suffisent plus Ã protÃ©ger les applications contre ces menaces de plus en plus persistantes.

Notre faÃ§on de travailler Ã©voluant quotidiennement, il s'avÃ¨re compliquÃ© pour les entreprises de maintenir une visibilitÃ© et un contrÃ´le constant sur son patrimoine documentaire. En effet, la multiplication des applications Cloud combinÃ©e Ã des connexions effectuÃ©es depuis n'importe quel appareil et de n'importe quel lieu renforce ce facteur risque.

Face Ã ce constat, Zscaler estime qu'en 2014 l'Ã©volution des menaces, la complexitÃ© du Cloud et les environnements mobiles seront intimement liÃ©s et met en exergue 5 thÃ¨mes majeurs

1/ L'importance du nom de domaine

Les attaques sur le nom de domaine sont en augmentation. Ceci s'explique par le fait que de nombreuses organisations n'ont aucune visibilitÃ© sur leur nom de domaine et que des dizaines de milliers de noms de domaines sur Internet ne sont pas sÃ©curisÃ©s.
Zscaler recommande une surveillance rÃ©guliÃ¨re du trafic, au moins une fois durant la semaine et mÃªme initier un paramÃ¨tre qui bloquerait l'accÃ¨s Ã tout site datant de moins de 24 heures.

2/ L'enchevÃªtrement du Web et de l'encodage SSL

Le dÃ©ploiement de services Cloud au sein des entreprises croÃ®t rÃ©guliÃ¨rement. L'encodage protÃ¨ge le trafic en transit mais le management est rendu difficile pour les services informatiques. Initialement, l'encodage SSL avait Ã©tÃ© conÃ§u pour Ã©changer 1024-bit. Dans le but de renforcer cet encodage, cela est passÃ© Ã 2048 bits Ã la fin 2013. La visibilitÃ© devrait Ãªtre alors cinq fois plus compliquÃ©e.
Le challenge de maintenir visibilitÃ© et contrÃ´le du trafic encodÃ© s'accÃ©lÃ¨rera en 2014, le rendant vulnÃ©rable aux hackers.

3/ Le BYOD est le maillon faible

Les appareils mobiles, de plus en plus utilisÃ©s, sont le nouveau point faible. Comme les entreprises migrent certaines de leurs donnÃ©es dans le Cloud et que les utilisateurs se connectent via des appareils mobiles, il n'existe plus de solution de sÃ©curitÃ© traditionnelle entre les donnÃ©es et l'appareil.

4/ MPLS va vers le Cloud Hybride : NetWork-Delivered Security

Les entreprises continuant globalement Ã grossir et Ã se tourner de plus en plus vers le Cloud, cela est devenu consommateur de temps, inefficace et coÃ»teux de dÃ©ployer de nouvelles solutions basÃ©es sur le Cloud par dessus des rÃ©seaux dÃ©suets. En 2014, Zscaler espÃ¨re voir les entreprises sÃ©curiser ses utilisateurs dans un Cloud hybride ou public plutÃ´t que de les laisser dans un rÃ©seau privÃ©.

5/ L'Internet des objets, cible de nouvelles attaques

L'Internet des objets possÃ¨de une maturitÃ© proche de celle du web de 1995. Ainsi, une personne malintentionnÃ©e qui piratera un rÃ©seau Wi-Fi ou dÃ©robera un smartphone, pourra ouvrir la porte du garage, Ã©teindre les camÃ©ras de surveillance, anÃ©antir les systÃ¨mes de sÃ©curitÃ©. En 2014, les pirates se pencheront sÃ©rieusement sur l'Internet des objets Ã la maison, au travail et dans des lieux sensibles.

L'intÃ©gralitÃ© de l'Ã©tude.

Pour de plus amples informations