Cloud Computing : Pour contrer au mieux les menaces informatiques.
Sécurité
Posté par : JerryG
Publiée le : 13/1/2014 15:00:00

Zscaler, acteur majeur dans les services de sécurité et de contrôle du trafic Web des entreprises, publie un document présentant ses prévisions 2014 quant à la sécurité dans le Cloud et met en avant **les écueils à éviter pour contrer au mieux les menaces informatiques.**
2013 aura été marquée par d'importantes cyber-attaques et il est justifié de dire qu'aujourd'hui les anti-virus classiques ne suffisent plus à protéger les applications contre ces menaces de plus en plus persistantes.

Notre façon de travailler évoluant quotidiennement, il s'avère compliqué pour les entreprises de maintenir une visibilité et un contrôle constant sur son patrimoine documentaire. En effet, la multiplication des applications Cloud combinée à des connexions effectuées depuis n'importe quel appareil et de n'importe quel lieu renforce ce facteur risque.

Face à ce constat, Zscaler estime qu'en 2014 l'évolution des menaces, la complexité du Cloud et les environnements mobiles seront intimement liés et met en exergue 5 thèmes majeurs

zscaler®
The Leader in Cloud Security

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 visibilité sur leur nom de domaine et que des dizaines de milliers de noms de domaines sur Internet ne sont pas sécurisés.
Zscaler recommande une surveillance régulière du trafic, au moins une fois durant la semaine et même initier un paramètre qui bloquerait l'accès à tout site datant de moins de 24 heures.

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

Le déploiement de services Cloud au sein des entreprises croît régulièrement. L'encodage protège le trafic en transit mais le management est rendu difficile pour les services informatiques.
Initialement, l'encodage SSL avait été conçu pour échanger 1024-bit. Dans le but de renforcer cet encodage, cela est passé à 2048 bits à la fin 2013. La visibilité devrait être alors cinq fois plus compliquée.
Le challenge de maintenir visibilité et contrôle du trafic encodé s'accélèrera en 2014, le rendant vulnérable aux hackers.

3/ Le BYOD est le maillon faible

Les appareils mobiles, de plus en plus utilisés, sont le nouveau point faible. Comme les entreprises migrent certaines de leurs données dans le Cloud et que les utilisateurs se connectent via des appareils mobiles, il n'existe plus de solution de sécurité traditionnelle entre les données et l'appareil.

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

Les entreprises continuant globalement à grossir et à se tourner de plus en plus vers le Cloud, cela est devenu consommateur de temps, inefficace et coûteux de déployer de nouvelles solutions basées sur le Cloud par dessus des réseaux désuets. En 2014, Zscaler espère voir les entreprises sécuriser ses utilisateurs dans un Cloud hybride ou public plutôt que de les laisser dans un réseau privé.

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

L'Internet des objets possède une maturité proche de celle du web de 1995. Ainsi, une personne malintentionnée qui piratera un réseau Wi-Fi ou dérobera un smartphone, pourra ouvrir la porte du garage, éteindre les caméras de surveillance, anéantir les systèmes de sécurité. En 2014, les pirates se pencheront sérieusement sur l'Internet des objets à la maison, au travail et dans des lieux sensibles.

L'intégralité de l'étude.

Pour de plus amples informations