



Entretien avec ...

Renaud Bidou, Directeur Technique de Deny All, le spécialiste européen du Firewall Applicatif

Le Cloud Computing constitue une énième révolution dans le domaine de la sécurité ?

Les innovations technologiques dans le domaine de l'informatique ont toujours posé de nouvelles problématiques de sécurité. Dans les années 90 l'adoption généralisée du protocole IP pour les réseaux a exposé de nombreuses faiblesses conceptuelles jusqu'alors peu exploitées. Internet a soudainement ouvert l'accès aux systèmes d'information des entreprises puis des particuliers, et la mobilité a augmenté dramatiquement la « surface d'attaque » exploitable.

Le Cloud Computing fait partie de ces (r)évolutions. En l'adoptant, l'entreprise confie tout ou partie de ses données et de leurs traitements à une chaîne de tiers dont la sécurité et l'organisation sont peu ou mal maîtrisées.

Le Cloud Computing s'appuie par ailleurs lui-même sur des technologies (telles que les Web Services ou la virtualisation) dont la sécurité repose sur des concepts différents de ceux appliqués dans les infrastructures physiques actuelles.

De nouvelles technologies de communication entre les applications font leurs apparitions. Leur sécurité est-elle maîtrisée ?

Le Cloud Computing généralise l'implémentation de communications de « machine à machine » via des protocoles automatisés, permettant l'interopérabilité de systèmes hétérogènes. La puissance fonctionnelle de ces « Web Services » repose sur des applications plus ouvertes et plus accessibles, sur la diffusion incontrôlée de modes opératoires et sur des formats de données variables. Ces caractéristiques, poussées à l'extrême à des fins d'automatisation et d'interopérabilité, offrent de nouveaux angles d'attaque.

En outre l'utilisation socle technologique connu (tel que le protocole HTTP comme base pour le transport des messages) laisse à penser que les problématiques de sécurité sont déjà prises en compte par les infrastructures existantes. Cette illusion de la sécurité est une menace considérable pour le Cloud Computing.

La sécurité est déléguée. Peut-elle pour autant être contrôlée ?

Le fait d'externaliser une proportion importante du système d'information peut présenter un avantage notable. Certaines structures ne disposent pas des moyens humains et financiers nécessaires à la mise en place d'une sécurité efficace. Le principe de la mutualisation des ressources inhérente au Cloud Computing offre dès lors la possibilité de se disposer de pôles d'expertise auprès de tiers. En revanche l'évaluation de cette expertise reste complexe à plusieurs titres. D'une part, il n'existe aujourd'hui aucune norme ni certification concernant spécifiquement les technologies et infrastructures du Cloud. D'autre part, les infrastructures de Cloud Computing sont, par essence, distribuées entre plusieurs acteurs. Ainsi il est nécessaire d'évaluer non seulement la sécurité du fournisseur de service mais également de l'ensemble des tiers intervenant dans la chaîne applicative, directement ou indirectement.