

Le SaaS, une issue pour la sécurité des données ?

-Pour l'instant combien de vos clients utilisent du SaaS pour sécuriser leurs données? Quelles parts de marché cela représente?

À l'heure actuelle, le développement du SaaS n'en est qu'à ses débuts, la part de marché n'est donc pas significative.

- Quand pensez-vous que cela va vraiment exploser? A votre avis 2008 est-elle l'année du SaaS ?

Il est toujours difficile de faire ce genre de prédiction, mais je pense effectivement que l'année 2008 verra une progression importante de l'utilisation de logiciels en mode SaaS.

-Y a-t-il des secteurs d'activité pour lesquels le SaaS s'impose plus naturellement? Les entreprises préfèrent-elles externaliser l'ensemble de leurs données ou seulement une infime partie ? Quelles sont les données les plus critiques?

Le SaaS s'impose beaucoup plus rapidement dans les petites entreprises, car elles sont plus flexibles et surtout parce qu'elles ne disposent en général pas des compétences internes pour administrer correctement des applications complexes. Les applications de type ERP, CRM, Outils collaboratifs sont d'ailleurs les plus utilisées dans le modèle SaaS, ces applications renfermant généralement des données très sensibles pour l'entreprise (fichier clients, propositions, prix de revient, ...)

-Quelles sont les questions qu'un responsable informatique doit se poser avant de migrer vers une approche SaaS?

La réversibilité (capacité à quitter le fournisseur SaaS tout en récupérant ses données) est assurément le point crucial dont il faut s'assurer quand on migre vers une approche SaaS.

La sécurité de l'information (Confidentialité, Intégrité, Disponibilité) est un autre sujet d'extrême importance.

-Que répondez-vous aux éditeurs de solutions de sécurité, (Kaspersky Symantec, Panda McAfee) qui considèrent que le SaaS est une aubaine pour les hackers en ce sens que toutes les données sensibles sont stockées dans un seul et même endroit? Selon-vous, en quoi le SaaS apporte-t-il plus de sécurité?

Je répondrais par une autre question: est-il plus facile de sécuriser des milliers de serveurs éparpillés dans des lieux différents ou un datacenter qui centralise les mêmes données ? Une très grande majorité des entreprises (notamment les petites et moyennes) n'ont pas accès à la compétence nécessaire pour sécuriser leur système d'information, l'approche SaaS devrait permettre à ces entreprises d'améliorer leur niveau de sécurité (pour peu que le fournisseur SaaS investisse largement sur la sécurisation du SI).

-Il semble que le principal frein à l'adoption du SaaS soit la responsabilité du prestataire? Exemple : les problèmes de la responsabilité en cascade dans plusieurs affaires aux États-Unis. Quelles sont les garanties que vous donnez à vos clients en cas d'une lourde perte de données? Dédommagements, compensation financière ?

Nous le savons tous la sécurité à 100% n'existe pas. Et, quand on arrive à des niveaux de 99% de sécurité, le moindre dixième de pourcent de gagné peut coûter très cher. C'est là que les assurances doivent prendre le relais.

Petit zoom sur Arkoon La société Arkoon a été créée en décembre 1999 à Lyon. Le métier d'Arkoon est de construire et de développer des solutions de sécurité informatique pour les entreprises. Arkoon n'est donc pas un fournisseur de solutions en mode SaaS mais nos produits sont utilisés pour sécuriser les applications en mode SaaS. Nous comptons environ 90 employés. Le siège social est à Lyon avec des agences commerciales à Paris, Milan et très bientôt en Espagne. Le chiffre d'affaires 2006 est de 11 millions d'euros pour 250.000 euros de résultat net (le CA 2007 sera annoncé le le 29 janvier), explique Daniel Fages, fondateur du groupe .