

### **La sécurité des applications en mode SaaS : un axe stratégique**

#### **Sécurité**

Posté par : JulieM

Publié le : 18/4/2016 13:00:00

La généralisation de l'utilisation des applications SaaS est aujourd'hui une réalité concrète. Dans ce contexte, les éditeurs sont amenés à faire évoluer leurs offres pour délivrer leurs services dans le Cloud. Amorcer cette transformation vers le SaaS puis savoir en tirer le meilleur parti met les éditeurs face à des défis majeurs, qu'ils soient financiers, techniques ou bien commerciaux. Au-delà des évolutions organisationnelles, le passage au SaaS implique des changements en matière de responsabilité vis-à-vis des clients, c'est pourquoi la notion de sécurisation se positionne désormais comme une donnée stratégique.

En effet, en proposant leurs offres en mode SaaS, les éditeurs vont devoir répondre à de nombreuses contraintes et prendre des dispositions pour proposer une qualité de service de premier plan ; que ce soit en matière de haute disponibilité, de sécurité des échanges de flux, de confidentialité des données archivées ;

Dans ce contexte, le choix de l'hébergeur est un élément clé. Considérant que les éditeurs de solutions SaaS doivent s'engager contractuellement sur de nombreux aspects dont la sécurité des données, il convient de cartographier précisément le dispositif de sécurité mis en œuvre par le prestataire d'hébergement pour garantir une parfaite sécurité des applications hébergées. À ce niveau, des qualités de service très différentes sont proposées. Attention à ne pas se tromper afin de ne pas avoir une qualité de service dégradée qui pourrait être reprochée à l'éditeur par ses utilisateurs.

Votre prestataire doit démontrer sa capacité à répondre aux enjeux suivants : protection et actions aux menaces liées à la cybersécurité, mise en œuvre des solutions rapides et efficaces, prévention des attaques par des tests réguliers des dispositifs mis en place.

Ses engagements contractuels doivent être mesurables, mesurés et adaptés à votre taille, à votre activité et à la criticité des données concernées. Il pourra par exemple proposer des SLA personnalisés, des pénalités associées, sans oublier de présenter les scénarios de réversibilité des données.

Au niveau de la confidentialité des données, il convient également de se pencher sur des aspects réglementaires et de vérifier qu'aucune législation particulière (au niveau de la nationalité de l'hébergeur et du lieu d'hébergement) ne compromet la confidentialité des données hébergées. Ce point a notamment fait couler beaucoup d'encre au niveau du Patriot Act aux États-Unis.

Enfin, il faut trouver un partenaire capable d'accompagner l'éditeur dans sa croissance. Ainsi, il est nécessaire de s'appuyer sur des structures pouvant vous proposer une offre adaptée à votre maturité dans le SaaS. Un éditeur qui démarre dans le Cloud cherchera à optimiser les coûts, à adapter les grilles tarifaires et les modèles de rémunération de ses commerciaux : il optera pour une offre évolutive fonction de l'acquisition de ses premiers clients en SaaS. Les éditeurs dont l'offre SaaS est mature et les pureplayers rechercheront plutôt un prestataire capable d'absorber une forte montée en charge en assurant une parfaite sécurisation des flux échangés et stockés.

Ces quelques éléments mettent en avant des notions fondamentales que les éditeurs vont

devoir intégrer dans la mise en œuvre de leurs modèles SaaS. Cela leur permettra de positionner la sécurité au centre de leur dispositif et de s'appuyer sur des hébergeurs prenant toutes les garanties nécessaires pour fiabiliser leurs infrastructures, affirme Virginie Kiener, Responsable Marketing de la business unit Aspaway (Groupe Claranet).