

Les 5 principales erreurs Ã ne pas commettre lorsqu'on adopte le Cloud
Internet

PostÃ© par : JPilo

PubliÃ© le : 12/4/2012 11:00:00

Cette annÃ©e, le **Cloud Computing gagne du terrain** au sein des entreprises. Les DSI sont dorÃ©navant convaincus que lorsqu'il est correctement implÃ©mentÃ©, le Cloud Computing peut radicalement amÃ©liorer la flexibilitÃ© et la productivitÃ© de lâ€™entreprise tout en rÃ©duisant les coÃ»ts dâ€™infrastructure.

On sâ€™attend Ã ce que les grandes et petites entreprises basculent dâ€™importantes parties de leurs opÃ©rations dans le Cloud dâ€™ici les deux prochaines annÃ©es.

Pourtant, alors que chaque organisation veut une partie du Cloud, toutes nâ€™obtiendront pas les rÃ©sultats quâ€™elles dÃ©sirent. Voici les cinq principales erreurs Ã Ã©viter, selon **Christophe Auberger**, Responsable Technique chez Fortinet

1. Ne pas opter pour le bon modÃ¨le de cloud



Les entreprises migrant vers le Cloud peuvent choisir parmi les Clouds publics, Clouds privÃ©s, Clouds communautaires ou Clouds hybrides.

1. Le Cloud public: Il appartient Ã un fournisseur Cloud et est accessible Ã un large public. Le principe est de payer Ã lâ€™utilisation et la plateforme est partagÃ©e avec dâ€™autres utilisateurs.

2. Le Cloud privÃ©: Il appartient et est dÃ©ployÃ© par une organisation pour sa propre utilisation puisquâ€™elle en est la seule et unique propriÃ©taire.

3. Le Cloud communautaire: Il est partagÃ© en coopÃ©ration par plusieurs organisations,

souvent de la même industrie.

4. Le Cloud hybride : Il mixe les modèles de déploiement Cloud Ã©numÃ©rÃ©s ci-dessus, permettant aux applications et donnÃ©es de passer facilement d'un Cloud Ã l'autre.

Chaque type de dÃ©ploiement en matiÃ¨re de Cloud a ses avantages. Les facteurs Ã considÃ©rer avant l'adoption sont : le niveau de criticitÃ© des applications que l'entreprise veut basculer dans le Cloud ; les questions de rÃ©glementation et de conformitÃ© ; les niveaux de services (SLA) nÃ©cessaires ; les modes d'utilisation selon les charges de travail ; et la maniÃ¨re dont les applications doivent Ãªtre intÃ©grÃ©es aux autres fonctions de l'entreprise.

2. Ne pas intÃ©grer la sÃ©curitÃ© Cloud dans sa politique de sÃ©curitÃ© d'entreprise

Vos politiques de sÃ©curitÃ© Cloud et sÃ©curitÃ© d'entreprise doivent Ãªtre intÃ©grÃ©es. Au lieu de crÃ©er une nouvelle politique de sÃ©curitÃ© pour le Cloud, renforcez plutÃ´t vos politiques de sÃ©curitÃ© existantes en considÃ©rant cette plateforme supplÃ©mentaire. Pour modifier vos politiques Cloud, vous devez tenir compte des facteurs suivants: oÃ¹ sont stockÃ©es les donnÃ©es, comment elles sont protÃ©gÃ©es, qui en a accÃ¨s, mais aussi la conformitÃ© avec les rÃ©glementations, et les niveaux de services SLA.

Lorsqu'elle est correctement effectuÃ©e, l'adoption du Cloud Computing peut Ãªtre une occasion d'amÃ©liorer vos politiques de sÃ©curitÃ© et votre position globale de sÃ©curitÃ©.

3. Compter sur la sÃ©curitÃ© de son fournisseur de services cloud

Ne pensez pas que vos donnÃ©es soient automatiquement sÃ©curisÃ©es parce que vous utilisez un fournisseur de services. Vous devez faire un examen complet de la technologie et des processus de sÃ©curitÃ© du fournisseur, et vÃ©rifiez la maniÃ¨re dont ils sÃ©curisent vos donnÃ©es et leurs infrastructures. Plus prÃ©cisÃ©ment, vous devriez examiner :

1. La transportabilitÃ© des donnÃ©es et applications: votre fournisseur vous permet-il d'exporter les applications, donnÃ©es et processus existants dans le Cloud? Pouvez-vous les importer de nouveau aussi facilement ?

2. La sÃ©curitÃ© physique des centres de donnÃ©es: Comment les fournisseurs de services protÃ©gent leurs centres de donnÃ©es physiques? Utilisent-ils des centres de donnÃ©es certifiÃ©s aux normes SAS 70 Type II? Comment leurs opÃ©rateurs de centres de donnÃ©es sont-ils formÃ©s et qualifiÃ©s ?

3. La sÃ©curitÃ© des accÃ¨s et des opÃ©rations: Comment votre fournisseur contrÃ´le l'accÃ¨s aux machines physiques? Qui est en mesure d'accÃ©der Ã ces machines, et comment sont-elles gÃ©rÃ©es ?

4. La sÃ©curitÃ© du centre de donnÃ©es virtuel: L'architecture Cloud est la clÃ© de l'efficacitÃ©. Sachez comment les parties individuelles telles que les nÃuds de traitement, nÃuds du rÃ©seau et nÃuds de stockage sont architecturÃ©s, et comment elles sont intÃ©grÃ©es et sÃ©curisÃ©es.

5. La sÃ©curitÃ© des donnÃ©es et des applications: Pour mettre vos politiques en application, la solution Cloud doit vous permettre de dÃ©finir des groupes et rÃ´les avec un contrÃ´le d'accÃ¨s basÃ© sur le rÃ´le prÃ©cis, des rÃ©gles de mots de passe et une encryption des donnÃ©es appropriÃ©es (en transit et Ã l'arrÃªt).

4. Supposer que vous n'Ãªtes plus responsable de la sÃ©curisation des donnÃ©es

Ne pensez jamais que l'externalisation de vos applications ou systèmes signifie que vous n'êtes plus responsable en cas de violation de données. Certaines PME ont cette fausse idée mais sachez que votre entreprise est toujours au bout du compte responsable vis-à-vis de ses clients et de tout autre partie prenante lorsqu'il s'agit de l'inviolabilité des données. Autrement dit, c'est votre CEO qui risque d'aller en prison, et non le fournisseur cloud.

5. Ne pas savoir quelles lois locales s'appliquent

Les données qui sont en sécurité dans un pays peuvent ne pas l'être dans un autre. Cependant, dans de nombreux cas, les utilisateurs des services Cloud ne savent pas où sont stockées leurs informations. Actuellement dans le processus d'harmonisation des lois sur les données de ses États membres, l'Union Européenne favorise la protection très stricte de la vie privée, tandis que les lois américaines, telles que l'US Patriot Act, permettent au gouvernement et autres organismes d'avoir un accès quasi illimité aux informations appartenant aux entreprises.

Sachez toujours où sont vos données. Si nécessaire, stockez vos données dans plusieurs endroits. Il est conseillé de choisir une juridiction qui vous permet d'accéder à vos données même si votre contrat avec votre fournisseur Cloud se termine de manière inattendue. Le fournisseur de services devrait également vous donner l'option de choisir l'endroit où vos données seront stockées.