Guides de sécurité pour les petites entreprises

Craintes pour la sécurité et cloud computing :
Instauration d'un climat de confiance envers les nouveaux modèles de fourniture de données

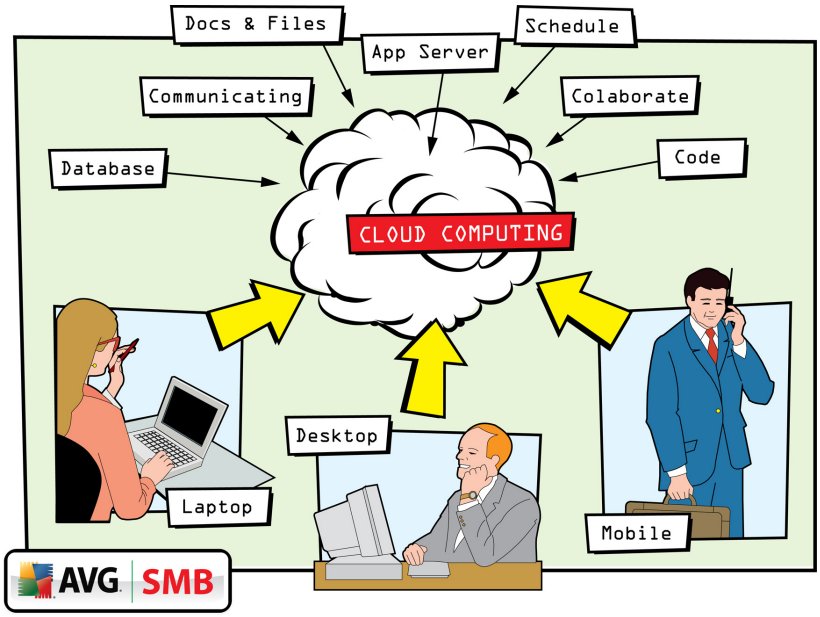
AVG AU TRAVAIL

Craintes pour la sécurité et cloud computing : Instauration d'un climat de confiance envers les nouveaux modèles de fourniture de données.

Le cloud computing pourrait radicalement transformer la manière dont les entreprises adoptent de nouvelles applications et augmentent leur puissance de calcul. Toutefois, il présente également de nouvelles menaces du point de vue de la sécurité.

Le cloud computing a été largement salué comme la « prochaine étape marquante » par les cercles technologiques. Dans le même temps, il a peut-être été décrit dans des termes exagérément compliqués.

Et si je vous disais que « Hotmail » est un bon exemple de cloud computing, est-ce que cela simplifierait les choses ? Ce concept est en réalité aussi simple qu'un utilisateur puisant dans un centre de données via sa connexion Internet afin d'accéder à un service en ligne, lequel, dans cet exemple, serait la messagerie Hotmail.



Développons cette définition tout en conservant sa simplicité. À mesure que notre utilisation du Web s'est étendue et que les pages Web elles-mêmes sont devenues plus dynamiques, la définition d'un service en ligne a évolué.

Alors que nous utilisions autrefois le Web pour trouver des informations, nous interagissons désormais directement avec Internet, car ses services ont évolué pour devenir des applications à part entière. Ces services présentent maintenant des fonctionnalités informatiques sous la même forme que celle que vous attendriez de votre propre PC.

Le saviez-vous :

- Le cloud computing est exposé aux mêmes problèmes de confiance que tout autre service technique, mais il y ajoute la complexité liée à une couche d'abstraction supplémentaire.
- S'il est correctement conçu et déployé, le cloud computing peut vous apporter de nouveaux flux de puissance de calcul, plus évolutifs.
- Une association à la pointe de la réflexion sur la sécurité, appelée Cloud Cube Model du Forum Jericho, présente les étapes que les entreprises devraient suivre avant de s'abonner à des services de cloud.
- La technologie de recherche et de navigation sécurisée AVG LinkScanner® (http://linkscanner.avg.com) peut appliquer plus de 100 indicateurs de menaces potentielles à une page Web.

Par conséquent, la puissance de calcul du cloud débute par un centre de données centralisé et est ensuite fournie aux utilisateurs à titre individuel ou groupée pour être proposée à une entreprise entière. Ce niveau de l'échelle informatique, dit niveau entreprise, est l'endroit où l'on pourrait utiliser le terme logiciel en tant que service, ou Saas (Software-as-a-Service).

Le cloud computing sans confiance n'est rien de plus qu'un épais brouillard

Si le cloud computing est fourni (et surtout, déployé) de manière intelligente, il transforme le jeu de manière positive, car il peut permettre de réaliser de véritables économies grâce au partage des ressources matérielles et logicielles qu'impose naturellement son utilisation. Ajoutez à ce fait l'efficacité qu'il peut offrir en termes de souplesse lorsque la demande en services informatiques augmente (ou diminue) et il apparaît clairement que ce paradigme informatique a un rôle important à jouer dans les centres de données modernes du monde entier.

Le problème ici tient au fait que le cloud computing vous oblige à faire confiance au fournisseur de services qui héberge le centre de données. Sans cette confiance, la sécurité n'est pas garantie.

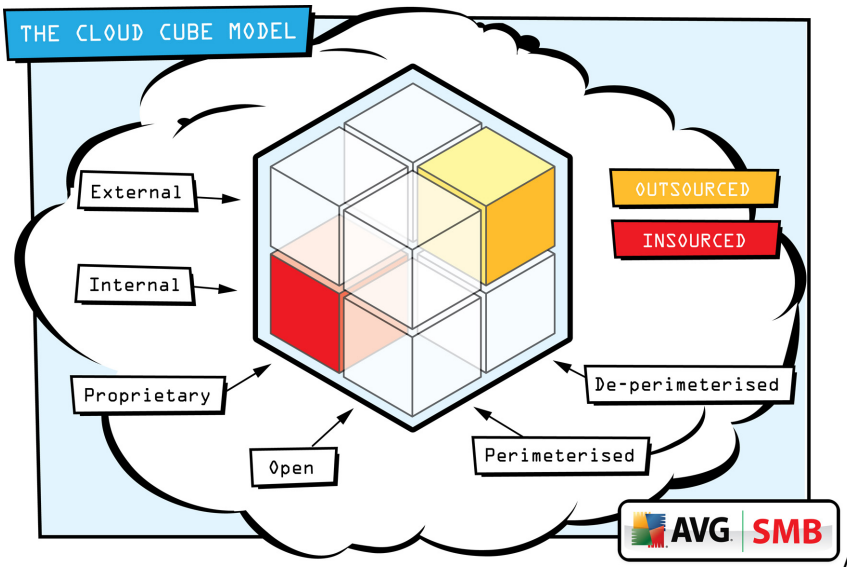
Dans ces conditions, comment progresser ? Et bien, même si le cloud computing en est encore (comparativement) au stade de l'adolescence, nous devons tenir compte de la quantité de donnée que l'entreprise sera exposée à une puissance de calcul externalisée.

Le gourou de la sécurité Bruce Schneier recommande un examen plus approfondi des problèmes de sécurité liés au déplacement des ressources vers le cloud. « La sécurité informatique est une question de confiance. Vous devez faire confiance à votre fabricant de processeurs et à vos fournisseurs de matériel, de système d'exploitation et de logiciels, sans oublier votre fournisseur de services Internet », explique Schneier sur son blog (http://www.schneier.com/essay-274.html) « Toutes ces personnes sont susceptibles de nuire à votre sécurité : mettre vos systèmes en panne, corrompre les données, permettre à un pirate d'accéder aux systèmes. »

« Lorsqu'un ordinateur est installé sur votre réseau, vous pouvez le protéger à l'aide d'autres systèmes de sécurité tels que des pare-feu et des systèmes de détection d'intrusion (IDS). Vous pouvez construire un système résistant qui fonctionnera, même si ces fournisseurs à qui vous devez faire confiance ne sont pas aussi fiables que vous le souhaiteriez », poursuit Schneier. « Avec tout modèle d'externalisation, qu'il s'agisse du cloud computing ou d'un autre, cela n'est pas possible. Vous devez faire pleinement confiance à votre prestataire de services. Il est essentiel non seulement de faire confiance à la sécurité du prestataire de service, mais aussi à sa fiabilité, sa disponibilité et ses procédures de continuité de l'activité. »

Comment entrer dans le cloud ?

Le Forum Jericho a élaboré une série de stratégies que les entreprises devraient adopter lorsqu'elles ont affaire à des fournisseurs de cloud computing. Ces stratégies sont regroupées dans ce que l'on appelle le Cloud Cube Model du Forum Jericho (www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf), qui discute des facteurs clés dont les entreprises devraient tenir compte avant de donner leur accord à un fournisseur ou un prestataire de services.



Adrian Secombe, membre du conseil d'administration du Forum Jericho et directeur de la sécurité des informations pour la société pharmaceutique Eli Lilly, explique : « L'approche par cloud de l'organisation de l'activité peut être à la fois plus sécurisée et plus efficace que la structure classique en silo.

« D'un autre côté, elle pourrait ouvrir une véritable boîte de Pandore de cauchemars de sécurité... portant notamment sur la perte de la confidentialité et de l'intégrité des données. »

« Une approche soigneusement analysée et sélectionnée de la mise en œuvre du cloud computing peut vous redonner le contrôle de ces problèmes de sécurité », ajoute Secombe. « Il est indispensable de bien comprendre les principes de base et chaque entreprise doit développer un modèle de cloud qui favorise la consumérisation, at-

ténue les coûts et réduit les risques. »

Outre les problèmes potentiels de confiance associés à la migration de la messagerie vers un prestataire de service géré hébergé, ce type d'applications en ligne ne semble pas présenter de menaces de sécurité particulières.

Toutefois, un logiciel antivirus à jour tel que AVG Anti-Virus Business Edition 2011 (http://www.avg.com/fr-fr/anti-virus-business) peut apporter une couche de protection précieuse aux systèmes stratégiques.

Le logiciel LinkScanner® (http://linkscanner.avg.com) d'AVG contribue également à prévenir les attaques sur le Web, lesquelles risqueraient d'être intégrées aux applications de cloud et aux sites Web associés. Selon AVG, LinkScanner® utilise une base de données de cloud pour déterminer si un site Web particulier héberge un code malveillant.

La société explique : « LinkScanner® peut appliquer plus de 100 indicateurs de menaces potentielles à une page ». « Si le résultat n'est pas concluant, LinkScanner® appelle le cloud pour vérifier une multitude de détecteurs d'hameçonnage connectés au réseau de recherche AVG afin de déterminer avec certitude le risque de menace. »

Même si le cloud ne s'avère pas finalement à la hauteur de toute la publicité qui l'a entouré, il semble s'agir de la manière logique de développer l'informatique de prochaine génération. On peut dire sans risque d'erreur que la plupart des entreprises adopteront tôt ou tard au moins certains aspects de ce modèle, surtout s'il se révèle plus économique et plus souple.

La nécessité de faire confiance à ceux qui fournissent le service de cloud s'impose comme une réalité incontournable, mais il semble également que les entreprises puissent prendre certaines mesures pour atténuer le risque, de la modélisation de haut niveau aux approches qui ont fait leurs preuves en matière de sécurité Internet et matérielle.

Que faire ?

- Consultez le modèle Cube de l'informatique cloud du Forum Jericho avant de conclure un accord avec un fournisseur ou un prestataire de services Internet
- Analysez la quantité de données que vous confieriez à des ordinateurs externalisés et le risque auquel cela exposerait votre entreprise
- Utilisez un logiciel antivirus à jour tel que AVG Anti-Virus Business Edition 2011 (http://www.avg.com/fr-fr/antivirus-business) pour protéger vos systèmes stratégiques.

AVG SMB group :
bit.ly/AVGSMB

Devenez fan d'AVG :
facebook.com/avgfree

Lisez nos blogs:
blogs.avg.com

Suivez-nous sur :
twitter.com/
officialAVGnews

Devenez un affilié AVG :
avg.com/gb-en/
affiliate

Regardez notre chaîne :
youtube.com/user/
officialAVG

AVG Technologies France
1, Place de la Chapelle
64600 Anglet
France
www.avg.fr

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
République Tchèque
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
États-Unis
www.avg.com/us-en/
homepage

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Royaume-Uni
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Allemagne
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosie, Chypre
www.avg.com

AVG AU TRAVAIL