

20/11/2009

www.enisa.europa.eu

ENISA dissipe le brouillard sur la sécurité du Cloud Computing

De quelle manière les entreprises et gouvernements peuvent-ils profiter des avantages évidents du Cloud computing sans mettre en danger leur organisation ? L'agence européenne de la « sécurité cybernétique » répond à cette question dans un nouveau rapport complet intitulé « Cloud Computing : avantages, risques et recommandations pour la sécurité de l'information ». Ce rapport couvre les implications techniques, politiques et juridiques et surtout donne des conseils concrets sur la manière de gérer les risques et de maximiser les avantages des utilisateurs.

Le nouveau rapport de l'ENISA est le premier à étudier en profondeur toutes les questions de sécurité et de respect de la vie privée en vue du passage au Cloud Computing, exposant certains avantages en termes de sécurité de l'information en ce qui concerne l'information via Internet, ainsi que les 35 risques en matière de sécurité. L'ENISA et son groupe d'experts ont commencé par une enquête demandant aux entreprises quelles étaient leurs principales préoccupations quant au passage à l'informatique au cloud computing. « Le tableau que nous en avons tiré est clair, déclare Giles Hogben, expert à l'ENISA et éditeur du rapport : l'étude de cas sur l'informatique cloud computing est transparente - c'est l'informatique à volonté, instantanément disponible, sans engagement et à la demande. Mais le problème numéro 1 qui retient de nombreuses personnes, est la sécurité - comment puis-je être sûr de la fiabilité de ce service et faire confiance au fournisseur de services informatiques via l'Internet en lui confiant mes données et même, dans certains cas, la totalité de l'infrastructure de mon entreprise ? »

Le rapport répond à cette question par une liste de critères détaillés que chacun peut utiliser pour déterminer si un fournisseur de services informatiques via l'Internet prend la question de la sécurité au sérieux. « Il s'agit du résultat le plus important de notre rapport : notre liste de points à vérifier n'est pas sortie du chapeau, déclare Daniele Catteddu, coéditrice du rapport de l'ENISA, nous l'avons basée sur une analyse de risques de plusieurs scénarios de Cloud Computing, en mettant l'accent sur les besoins des clients de l'entreprise. Les risques les plus importants abordés dans la liste des points à vérifier incluent le verrouillage, les erreurs mécaniques dans la séparation des données clients et des applications, et les risques juridiques comme le non-respect de la conformité à la législation sur la protection des données ». Grâce à cette liste de points à vérifier sur la sécurité, les clients savent maintenant quelles sont les questions à

20/11/2009

www.enisa.europa.eu

poser et les prestataires de services peuvent répondre à ces questions une fois pour toutes au lieu d'être dépassés par les demandes de garantie sur leurs pratiques en matière de sécurité.

Le Cloud Computing implique également des intérêts économiques importants comme les prévisions d'IDC annonçant une croissance des services d'informatique cloud computing de 971 millions d'euros en 2008 à 6 005 millions en 2013.

Mais comme le rapport le souligne, le Cloud Computing est également un facilitateur de sécurité. Udo Helmbrecht, Directeur Exécutif de l'ENISA, souligne : « La capacité et la flexibilité de l'informatique cloud computing donnent aux fournisseurs un plus à la sécurité. Par exemple, les fournisseurs peuvent instantanément faire appel à des ressources supplémentaires défensives comme le filtrage ou le re-routage. Ils peuvent également déployer de nouveaux patches de sécurité de manière plus efficace et conserver plus de preuves de diagnostics » .

Téléchargez le rapport complet sur :

<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>

ENISA - European Network and Information Security Agency

Pour convenir d'une interview : Ulf Bergstrom, Chargé Relations Presse & Communication, ENISA, press@enisa.europa.eu, Portable : +30-6948-460143