Le Fonds Européen de Développement Régional et la Région wallonne investissent dans votre avenir

Rewics (04 mai 2011) - Atelier : « *L'informatique dans les nuages (cloud computing) : vraie révolution ou pétard mouillé ?* »

The Dark Side Of The Cloud

Robert Viseur (*robert.viseur@cetic.be*)

www.cetic.be

Your connection to ICT research

Qui suis-je?

- Nom : Robert VISEUR (www.robertviseur.be).
- Formation : Ingénieur civil en Informatique et Gestion (AIMs) et Docteur en Sciences Appliquées.
- Activités professionnelles :
  - Ingénieur de recherche senior au CETIC (www.cetic.be).
  - Assistant dans le service d'Économie et de Management de l'Innovation de la Faculté Polytechnique de Mons (mi.fpms.ac.be), UMons (www.umons.ac.be).
- Compétences : ebusiness, management de l'innovation, management Open Source (modèles d'affaires, valorisation, sélection de technologies,...), moteurs de recherche (API, indexation fulltext,...),...

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

Sécurité

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

Les inquiétudes sont-elles fondées ?

- Selon Forrester, 68% des DSI émettent des inquiétudes quant à la sécurité des clouds.
- Il y a eu des précédents pour renforcer ces craintes :
  - Cheval de Troie Zbot (Zeus) contre Amazon EC2 (botnet).
  - Opération chinoise (?) Aurora contre Google (mais aussi Symantec, Adobe Systems, Morgan Stanley,...).
    - Principe : exploitation d'une faille d'Internet Explorer permettant l'installation d'un malware et, ensuite, l'accès à l'Intranet de Google.
  - Gigapanne sur Amazon (21 avril 2011) :
    - Services affectés : Amazon EBS sur EC2 et Amazon RDS (utilisation d'EBS pour le stockage).
    - 3 jours de très fortes perturbations sur la zone « US East Region ».
    - 0,07% des données perdues (mais réelle transparence d'Amazon).
    - Cause : erreur humaine (routage) lors d'une mise à jour (pas de problème de sécurité à proprement parler) -> audit interne annoncé en réaction.

Quelle est la typologie des clouds ?

- Il y a cloud et cloud :
  - Clouds privés.
    - Internes à l'entreprise.
  - Clouds publics.
    - Externe à l'entreprise (externalisation vers un hébergeur).
    - Exemple : Microsoft Azure, Amazon EC2, Google App Engine,...
  - Clouds hybrides ou mixtes.
- L'utilisation d'un cloud n'implique donc pas obligatoirement le recours à un réseau de machines extérieures au SI de l'entreprise.

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

Quelle est la typologie des risques ?

- Risques internes (~70%).
  - Exemple : expédition d'un document confidentiel au mauvais destinataire, vols de fichiers (copie sur clef USB, piratage de copieurs informatiques,...),...
- Risques externes (~30%).
  - Attaques sur les postes de travail (~70%).
    - Attaques ciblées sur Adobe Acrobat Reader, sur Internet Explorer, sur Microsoft Office, sur les extensions Active X,...
    - Exemple : récente attaque sur Bercy en France (G20 2011) via un cheval de Troie associé à un fichier PDF.
  - Attaques sur les serveurs (~30%).
    - Exploitation de vulnérabilités des systèmes d'exploitation, de serveurs Web, de serveurs de bases de données, d'applications ou d'erreurs de configuration,...
- Sources : CERT-IST, Evidian (Bull), CNILL,...

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

Quels sont les problèmes de sécurité associés aux clouds ?

- Risque d'attaque interne (malveillance) ou externe (exploitation de faille concernant directement ou indirectement l'infrastructure) sur l'hébergeur.
  - Risque lié à la localisation des données et des logiciels (espionnage industriel, contrefaçons, saisies judiciaires,...).
- Risque d'usurpation d'identité (connexion).
  - Opérations de hameçonnage (*phishing*).
- Risque d'indisponibilité (attaque DDOS sur l'hébergeur,...).
  - Autres causes : indisponibilité réseau, bug, erreur humaine,...
- Quels sont réellement les moyens mis en œuvre par l'hébergeur (protections techniques, procédures internes, sauvegarde, disponibilité,...) ?
  - « *La sécurité obtenue en cachant les risques n'est qu'un leurre* ».

Protection de la vie privée

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

Quels sont les problèmes liés à la protection de la vie privée ?

- Risque de vol de données (exemple : clients, patients,...).
  - Causes possibles : accès aux données en interne, cloud pas sécurisé, application souffrant de failles de sécurité,...
- Ne pas oublier la responsabilité du client aux yeux de la loi : mise en œuvre de mesures de protection proportionnées à la nature des données (anonymisation, chiffrement,...), séparation physique de certains types de données,...

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

Propriété des données

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

Quels sont les problèmes liés à la propriété des données ? (1/2)

- Que spécifie le contrat vous liant à l'hébergeur (conditions générales d'utilisation) ? Qu'est-il prévu à la fin du contrat vous liant à lui ?
- Quelle maîtrise avez-vous réellement sur vos données ?
  - Récupération et exploitation de données.
    - Exemple d'engagement : « TIO Libre Definitions ».
      - OPENESS : data freedom.
      - FREE : data freedom, software freedom, competition freedom).

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

Quels sont les problèmes liés à la propriété des données ? (2/2)

- Quelle maîtrise avez-vous réellement sur vos données (suite) ?
  - Problème d'intéropérabilité entre clouds.
    - Efforts en matière de standardisation.
    - Présence de plusieurs organismes (*Open Grid Forum*, *Distributed Management Task Force*, *Cloud Security Alliance*,...).
    - Exemples (logiciels) :
      - OpenStack (Open Source) : technologie pour la mise en oeuvre de clouds privés compatible avec différentes briques logicielles existantes.
      - Deltacloud (Open Source, incubateur Apache) : API REST permettant l'accès uniformisé à différents technologies clouds (Amazon, Red Hat,...).
- Question supplémentaire de l'accès aux données par les autorités (actions en justice).

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

Conclusion

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

A quoi dois-je faire attention ?

- Faites attention aux dispositions prévues dans le contrat vous liant à l'hébergeur (garanties de performance, responsabilités, propriété des données,...).
- Faites attention à la crédibilité des promesses faites par l'hébergeur (moyens mis en œuvre).
- Faites attention à la propriété des données ainsi qu'aux possibilités de migration des données et des logiciels (interopérabilité).
- Faites attention à vos procédures et outils internes (règles d'accès aux données clients, procédure d'authentification,...)...
- Posez vous la question du niveau de risque que vous êtes globalement prêt(e)s à prendre et...
- Ne surestimez pas, en comparaison, vos propres capacités en gestion de systèmes d'information!

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

cetic

Avec le soutien de l'Union européenne et de la Région wallonne

Merci pour votre attention

Contact: Robert VISEUR (*robert.viseur@cetic.be*)

www.cetic.be

Your connection to ICT research