Cloud

Cedric Foll / @follc

Responsable infra @université Lille 3
Rédacteur en chef de #MISCMag

Cloud

- Le Cloud?
- Elements juridiques et réglementaires
  - PSSIE, Cloud souverain, Patriot Act
- La sécurité du cloud
  - Disponibilité / Intégrité / Confidentialité
  - Organisationel
- Les enjeux pour les DSI et RSSI
  - Opportunité
  - Maitriser les usages

Le Cloud?

Les offres:

- SaaS
- PaaS
- IaaS
- Housing

Software as a Service

- Mise à disposition d'une application en ligne
  - Tendance lourde du marché suivie par les éditeurs historiques tels que Microsoft & Adobe
  - A la fois des offres grand public et professionnel.
- Le fournisseur de service s'occupe de tout
  - D'où le succès auprès du grand public
- Exemples
  - Grand public: DropBox; Google docs, …
  - Professionel: Office 365, Google Apps

Plateform as a Service

- Mise à disposition de middleware pré-configuré
  - Evolution des hébergements web mutualisés.
  - A la fois des offres grand public (pour utilisateurs avertis) et professionnelles.
- Le prestataire met à disposition l'OS et le middleware (base de données, serveur d' application, …), le client gère l'application
- Exemples:
  - Hébergement web PHP/MySQL, Googles Apps, Microsoft Azure Web Services

Infrastructure as a Service

- ``Mise à disposition de VM (ou de serveur physique) et d'espace de stockage associé
  - Pour les petites entreprises offres très concurrentielles
    - Plus besoin de data center (salle blanche, climatisation, onduleurs, groupes éléctreogènes, …)
    - Achat de puissance (ram, CPU, surface de stockage) à la demande, plus d'investissement informatique.
  - A la fois des offres grand public (pour utilisateurs avertis) et professionnelles.
- Grande variété des offres
  - VPS d'OVH à 1,99€/mois/VM
  - Des serveurs physiques avec`couche de virtualisation associée peuvent se chiffrer à plusieurs k€/mois.

Housing ou hébergement sec

- Location de mètres carrés dans un Datacenter
  - Le prestataire fournit les rack, l'éléctricité (avec onduleur, groupe éléctrogène), la climatisation et la connectique réseau.
  - Le client achète ses propres serveurs, SAN, équipements réseaux, qu'il dépose chez l' hébergeur.
  - Type d'offre dédiée aux professionnels
  - Facturé au nombre de "U" dans les baies et à la consommation éléctrique.
- Part du constat qu'un hébergement avec un fort SLA c' est très cher, nécessite des compétences particulières (éléctricité, climatisation) et doit être sur plusieurs

Considérations juridiques

- Hébergement aux US (ou par une société US):
  - Patriot Act: Dans le cadre de la lutte contre le terrorisme toute entreprise américaine doit fournir les «données sensibles» demandées par l'administration fédérale, même si celles-ci sont stockées en Europe. Les entreprises visées n'ont pas le droit de communiquer sur la question.
  - Affaire Microsoft 2014: Si une société est américaine, elle doit fournir toute donnée demandée par la justice américaine même si celle-ci est stockée en dehors des US (voir article de Tris Acatrinei dans MISC 76).
  - PRISM: La NSA a directement accès aux données d'une centaine d'entreprises US dont Microsoft, Google, Facebook.
  - Upstream: La NSA écoute et analyse le trafic des principaux liens passant par les US.

Réglementation francaise

- Pour les administrations:
  - PSSIE de l'ANSSI publiée l'été 2014:

    " Les informations de l'administration considérées comme sensibles, en raison de leurs besoins en confidentialité, intégrité ou disponibilité, sont hébergées sur le territoire national."
  - Il faut donc recourir à un prestataire français avec infrastructures françaises et localisation française :
    - Ce qui limite énormément les choix, en particulier interdiction de recourir aux offres Google, Microsoft, Amazon, …
    - Le Cloud "souverain" c'est VMWare, HP, Cisco, Checkpoint, Fortinet et F5 http://www.journaldunet.com/solutions/cloud-computing/comparatif-cloudwatt-numergy-clouds-souverains/numergy.shtml
  - Guide de bonnes pratiques en cours de rédaction par l'ANSSI http://www.ssi.gouv.fr/fr/menu/actualites/appel-commentaires-referentiel-d-exigences-informatique-nuage.html

Eléments de sécurité

- Tryptique Disponibilité/Intégrité/Confidentialité?
  - Disponibilité:
    - Dépend du SLA de prestataire: vérifier qu'il est en accord avec celui exigé par les MAO.
      - Les offres grand publique n'ont pas de SLA (ie ça marche la plupart du temps, quand c'est en panne il faut attendre).
      - Dans les offres professionelles, un SLA important induit un surcout (GTR, GTI, disponibilité).
    - Dépend aussi du SLA de son fournisseur d'accès: en cas de panne du lien WAN, plus d'applications…
    - Réversabilité
      - Comment les données stockées chez le prestataire vont pouvoir être récupérées en fin de contrat? Comment gérer le basculement vers un nouveau prestataire ou une réinternalisation?
      - Que faire si le prestataire cesse ses activités? Faillite, abandon d'une solution, ...

Eléments de sécurité

- Intégrité
  - Sauvegarde et restauration des données
    - Service intégré à l'offre? En générale possible avec surcout.
- Confidentialité
  - Le prestataire peut techniquement accéder à vos données.
    - Malveillance, espionnage industriel,
  - Sécurité des accès aux interfaces d'administration du prestataire
    - http://www.lemondeinformatique.fr/actualites/lire-base-de-donnees-des-clients-europe-d-ovh-piratee-54482.html
  - Failles dans le mécanisme l'isolation des VM
    - http://www.silicon.fr/faille-critique-xen-cloud-amazon-rackspace-touches-97142.html
  - Gestion des disques:
    - Les disques HS sont ils détruits?

Eléments de sécurité

- Organisationnel
  - Perte de maitrise de son système d'information
    - Ne pas considérer que le bénéfice financier à court terme.
    - Risque de dépendance très forte au prestataire de Cloud.
  - Les maintenances programmées sont décidées par le prestataire et non par vos contraintes métiers.
  - Attention aux offres grands publiques!
    - Pas de service VIP à quelques d'euros mensuel.
    - Les demandes d'une direction générale sont traitées avec la même priorité que celles d'un client lambda.
  - Possibilité de réaliser un test d'intrusion?

Opportunité

- Faire attention aux coûts cachés
  - SLA, sauvegarde, …
- Analyser les risques et avoir une vision à long terme:
  - Reversibilité des données, dépendance vis à vis du fournisseur, …
- Atouts du Cloud
  - La mutualisation des coûts permet de disposer d’ une infrastructure qu’une petite structure ne pourrait pas s’offrir.
  - Fléxibilité: puissance et stockage à la demande.
  - Plus besoins d’éléctriciens et climatiseurs pour le Data Center (IaaS / Housing).
  - Ni d’informaticiens (SaaS / PaaS)

Maitriser les usages

- Gestion de la fuite des utilisateurs de son SI vers le Cloud grand public
  - Utilisation de gmail pour l'accès aux messages professionels
  - Stockage des documents internes sur DropBox
  - Utilisation de skype pour les visio conférences
- Risques:
  - Fuite de données confidentielles
  - Perte de maitrise du SI
    - Que faire si l'utilisateur a un problème avec Skype? (perte identifiant, saturation d'un lien, …)
    - Positionnement du HelpDesk

Maitriser les usages

- Pistes pour réduire cette fuite
  - Interdire l'usage de solutions de Cloud grand public au travers de la PSSI
    - Fonctionne si vos usagers sont disciplinés…
    - Au moins les sensibiliser sur les risques: pas de sauvegarde, impossibilité de garantir le fonctionnement, confidentialité, …
  - Bloquer techniquement l'usage
    - Par le verrouillage des postes de travail (ie interdiction d'installer Skype)
    - Filtrage des flux réseaux
      - Fonctionne tant que le poste est dans le réseau d'entreprise
  - Mise à disposition d'outils internes performants...

Questions