Development institute international

5ème Conférence Annuelle

Traitement des Données Personnelles 2012

Paris, le 18 janvier 2012

Les enjeux de protection des données dans le CLOUD COMPUTING

Xavier AUGUSTIN
RSSI

Patrick CHAMBET
Architecte Sécurité du SI

Bouygues Telecom

Sommaire

- Présentation de Bouygues Télécom
- Présentation de la sécurité chez Bouygues Télécom
- Présentation technique du Cloud Computing (Patrick CHAMBET)
- Le point de vue du RSSI (Xavier AUGUSTIN)

Bouygues Telecom: chiffres clés

- Ouverture commerciale : **29 mai 1996**
- Acquisition d'un réseau fixe (FAI) : **1er juillet 2008**
- **11 187 000 clients** sur le **Mobile** (fin juin 2011)
- **1 023 000 de clients** sur le **Fixe** (fin juin 2011)
- **9 200** collaborateurs (fin 2010)
- **N° 1 de la relation client** Fixe et Mobile
- 14 années d'innovation

Le forfait

Le répondeur gratuit

Les offres illimitées Millennium

Bbox

Internet - tv - téléphonie

Bbox fibre

Internet - tv - téléphonie

1996 1997 1999 2002 2005 2006 2007 2008 2009 2010

Development institute international

L'organisation de la sécurité/conformité CNIL

- Direction générale
- Direction financière
- Direction des risques
  - **Direction sécurité**
- Direction informatique
  - **RSSI/CNIL**
  - Sécurités opérationnelles
- Direction réseau
  - **Sécurité réseau**

Sommaire

- Présentation de Bouygues Télécom
- Présentation de la sécurité chez Bouygues Télécom

➔ **Présentation technique du Cloud Computing (Patrick CHAMBET)**

- Le point de vue du RSSI (Xavier AUGUSTIN)

Qu'est-ce que le Cloud Computing ?

- Définition
  - Capacités informatiques (logiciel, plate-forme, CPU, stockage, …) délivrées comme des services à la demande
- Particularités
  - Accès distant (réseau)
  - Pas de visibilité sur l'infrastructure sous-jacente (d'où le terme « nuage »)
    - ➔forte mutualisation des ressources
  - Standardisation
  - Facturation à l'usage, avec de gros écarts possibles

Qu'est-ce que le Cloud Computing ?

- 3 types de services
  - SaaS (Software as a Service)
    - Ex: CRM (SalesForce), Google Apps, Office 365
  - PaaS (Platform as a Service)
    - Ex: site Web packagé Apache + PHP + mySQL
  - Iaas (Infrastructure as a Service)
    - Ex: machines virtuelles « nues » crées à la demande

Qu'est-ce que le Cloud Computing ?

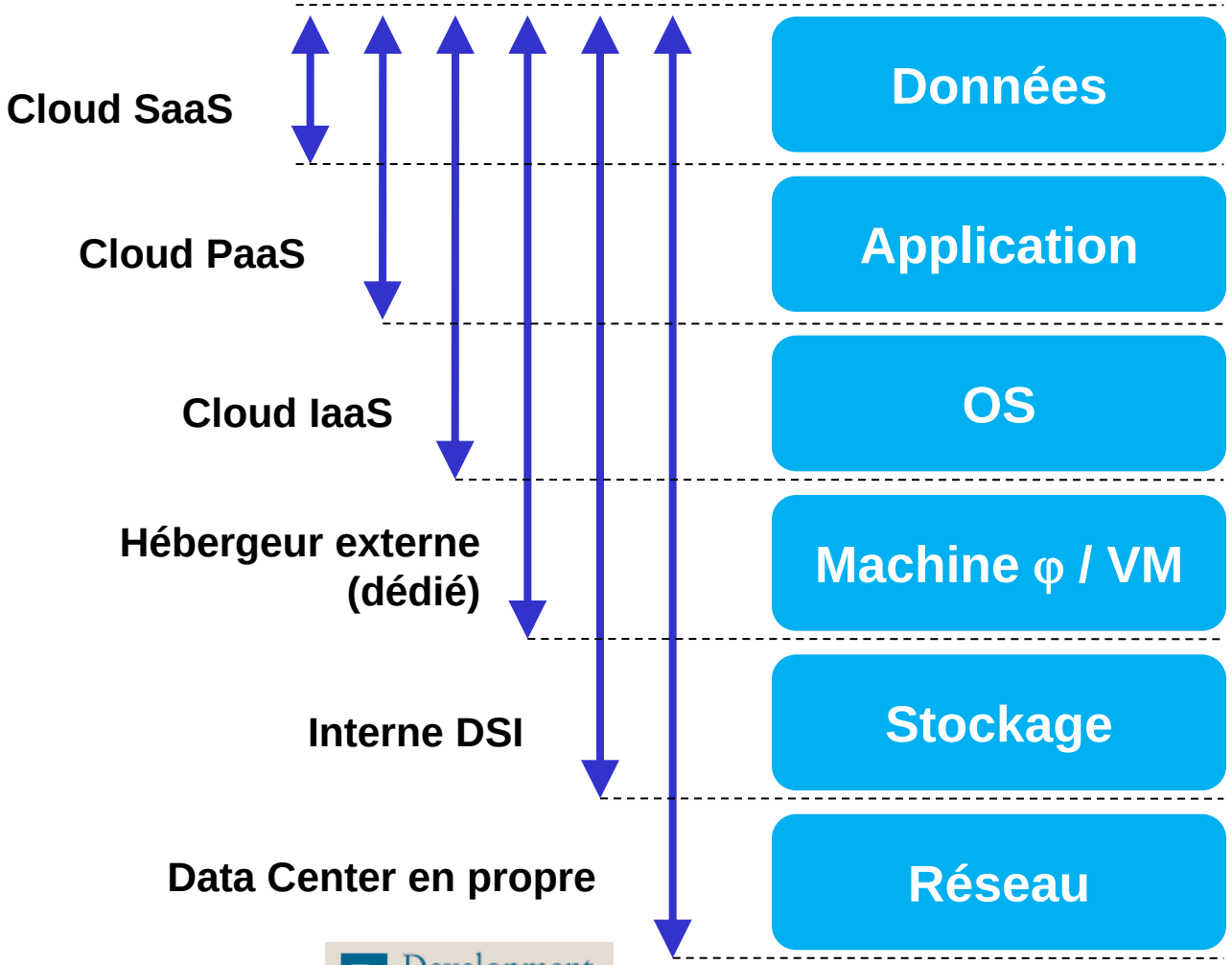
- 2 grandes catégories
  - Cloud public (on partage l'infra avec d'autres)
  - Cloud privé (on partage « peu » de choses)

- 2 localisations
  - Cloud externe (chez un fournisseur de Cloud)
  - Cloud interne (dans sa propre DSI)

➔ 4 possibilités

Vue technique du Cloud Computing

- Degré de contrôle de l'entreprise



Cloud Computing: les problématiques de sécurité

- Sur les données
  - Dépendent du choix des données mises dans le Cloud
  - De la localisation des données
    - Duplication, dispersion, lieux géographiques hors UE, …
  - Des contraintes légales
    - Paquet télécom: notification des violations de données personnelles
    - Réquisitions judicaires: comment y répondre ?
  - Protection des données
    - Qui peut y accéder (personnel du fournisseur, autres clients) ?

- Sur les applications
  - Qui a accès à quoi ?
    - Profils d'utilisateurs
  - Traçabilité des accès et des actions
    - Qui a fait quoi, quand, sur quelle donnée, depuis où ?

Cloud Computing: les solutions de sécurité

- Localisation des données
  - Savoir localiser géographiquement ses données
    - Pouvoir assurer à ses clients que leurs données sont stockées dans l'UE ou le groupe de l'article 29
  - Savoir s'assurer de la purge (destruction sécurisée) des données clients (à tous leurs emplacements)
  - Planifier la récupération d'informations en cas de saisie judiciaire (ex: messagerie hébergée dans le Cloud)
  - Prévoir la réversibilité

Cloud Computing: les solutions de sécurité

- Protection des données
  - Chiffrement des données
    - Dans les bases de données
    - Dans les fichiers
  - Chiffrement transparent
    - Chiffrement « à la volée » par l'application ou la base de données: facile en mode SaaS
    - Les clés de chiffrement sont forcément stockées dans le Cloud
    - Difficile d'interdire l'accès des administrateurs du Cloud aux clés
  - Chiffrement de bout en bout
    - Les clés sont détenues par les clients finaux
    - Le fournisseur de Cloud ne peut pas déchiffrer les données
    - Mais nécessite un client lourd ou un proxy de chiffrement (difficile en mode SaaS)

Cloud Computing: les solutions de sécurité

- Authentification des utilisateurs
  - Authentification nominative
  - 3 solutions
    - 2 annuaires distincts (entreprise + Cloud) avec synchronisation
    - Délégation d'authentification
    - Fédération d'identités (SAML, WS-Fédération, …)

Action nécessaire de la DSI

- Habilitation et contrôle d'accès
  - Mise en place de permissions d'accès fines sur les ressources et les données
  - Interdire les comptes génériques et le partage de comptes

Cloud Computing: les solutions de sécurité

- Traçabilité
  - Deux types de besoins
    1. Surveillance des accès aux ressources dans le Cloud
    2. Enquête / forensics en cas d'incident

  - Recueillir des traces suffisamment complètes (centraliser ou croiser les journaux de logs)
  - Protéger l'accès aux traces par le fournisseur de Cloud
  - Organiser la consultation ou la transmission des logs au client du Cloud
  - Prévoir la purge des logs au-delà d'une certaine période

Sommaire

- Présentation de Bouygues Télécom
- Présentation de la sécurité chez Bouygues Télécom
- Présentation technique du Cloud Computing (Patrick CHAMBET)

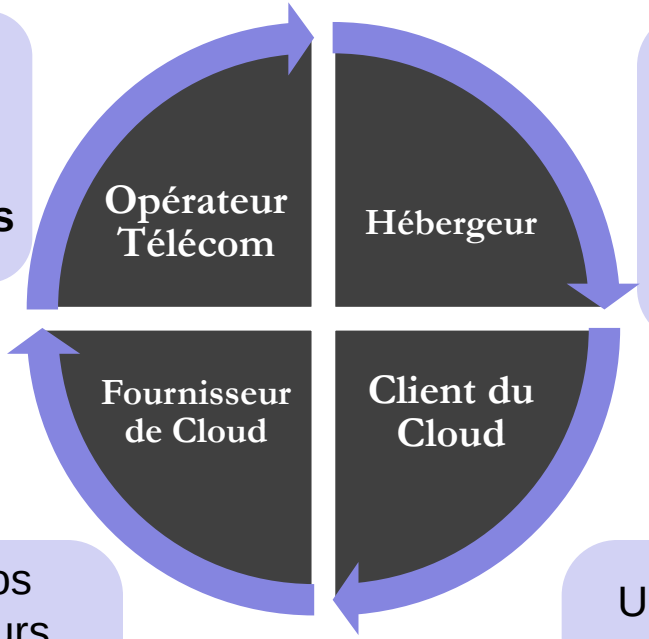
➔**Le point de vue du RSSI (Xavier AUGUSTIN)**

Le point du vue du RSSI

- Une vision large du Cloud (à la fois opérateur télécom, client et fournisseur)
- Une démarche responsable et prudente en tant qu'opérateur télécom et client du Cloud
- Une confiance client à développer en tant que fournisseur de Cloud (vision symétrique de la sécurité par rapport à nos obligations d'opérateur)

Opérateur, Client et Fournisseur

Une obligation de sécurité et de protection des données personnelles (OIV)



L'hébergement est notre métier
Une technologie nouvelle qui doit être maîtrisée

Un service proposé à nos clients et fondé sur la leurs confiance
Une offre qui doit être à la hauteur de nos propres attentes

Une opportunité pour nos métiers internes que la DSI doit accompagner
La protection des données personnelles est une obligation

En tant que client du Cloud

- Une attractivité et un intérêt évident pour les métiers
  - Accompagner le Cloud (sécurité)
  - Ou le concurrencer !
- Les applications cœur de métier seront a priori peu concernées (standardisation)
- **Une obligation de protection des données**
  - Sont-elles localisées ? Où ?
  - Sont-elles sécurisées ? (certification / clauses contractuelles types / une sécurité sur mesure)
  - Sont-elles protégées ? (information des personnes, droit d'accès, d'opposition, respect des durées de conservation, respect des finalités)
- **Un pré requis sur la localisation, la sécurité et la PVP => pas de données personnelles dans le nuage**
- Une clarification nécessaire de la CNIL - consultation en cours (localisation, sous-traitance en cascade et juridiction applicable).

En tant que fournisseur de Cloud

- Préserver et développer la relation de confiance avec nos clients (entreprise)
- Maîtriser la technologie (c'est aussi un bénéfice pour du Cloud interne et une vision symétrique de la protection des données)
- Un engagement fort sur la protection des données personnelles:
  - Localisation (en France)
  - Clauses contractuelles (type)
  - Mesure de sécurité
    - Cloisonnement des données
      => Contrôle d'accès (pas simple)
      => Chiffrement (transparent / applicatif)
    - Robustesse aux attaques Web (important)
    - Robustesse de l'exploitation (une technologie nouvelle)
- Sans oublier la disponibilité des applications , la continuité d'activité et la réversibilité)

Questions ?