LEXSI

INNOVATIVE SECURITY. FOR BUSINESS

Conseil / Audit / Formations
Veille et lutte contre la cybercriminalité

PANORAMA DES MENACES ET RISQUES POUR LE SI

CNIS EVENT

LEXSI > CNIS EVENT

05/11/2013

LEXSI

cnis EVENT
Computer, Network & Information Security

SOMMAIRE

BIG DATA

Définition

- Chaque jour, 2,5 trillions d'octets de données sont générées ;
  - Données les plus demandées : documents (84%), transactions commerciales (82%), emails (74%) Étude IDC-EMC « Extracting value from chaos » citée par Delphine Cuny sous le titre « "Big data" : la nouvelle révolution », Virginia Rometty, La tribune, nº 42, 29 mars au 4 avril 2013, p. 4
- Impossibilité de traiter une telle masse d'information avec des outils classiques ;
- Utilisation d'un modèle mathématique pour récupérer, analyser et synthétiser les informations ;
  - Ces analyses complexes répondent à la règle des 3V : Volume, Vélocité, Variété
  - Le Big Data est différent du Business Intelligence ;
- Utilisé à deux fins : commerciale ou aide à la décision

Selon McKinsey, une entreprise utilisant pleinement le *Big Data* pourrait augmenter sa marge opérationnelle de 60%

Big Data : the next frontier for innovation, competition and productivity, McKinsey Global Institute, Mai 2011

BIG DATA

Problématiques

- Quelle puissance de calculs ?
  - Pour des petites structures : cette puissance est disponible dans le Cloud : nécessite d'envoyer dans le Cloud des informations confidentielles
  - Obstacle perçu comme le plus important par 59% des personnes interrogées par Intel.
- Comment traiter l'information personnelle ?
  - Problème concernant le particulier
  - Mais qui peut impacter l'organisation : CNIL
- Que faire de mes algorithmes ?
  - Conservation / Confidentialité des algorithmes
- Comment m'assurer que les informations sont fiables ?

Récupérer un maximum de données tout en sécurisant ses propres données

BIG DATA

Risques

- Récupération de données confidentielles par des concurrents

- Défiance des individus

- Mauvais choix stratégiques

- Perte de l'avantage dans l'analyse des données

BIG DATA

Conclusion

Réglementaire

- Réglementation en constante évolution
- Globalisation de la législation

Implémentation

- Ce n'est pas tant un sujet technique qu'organisationnel

Protection de la donnée

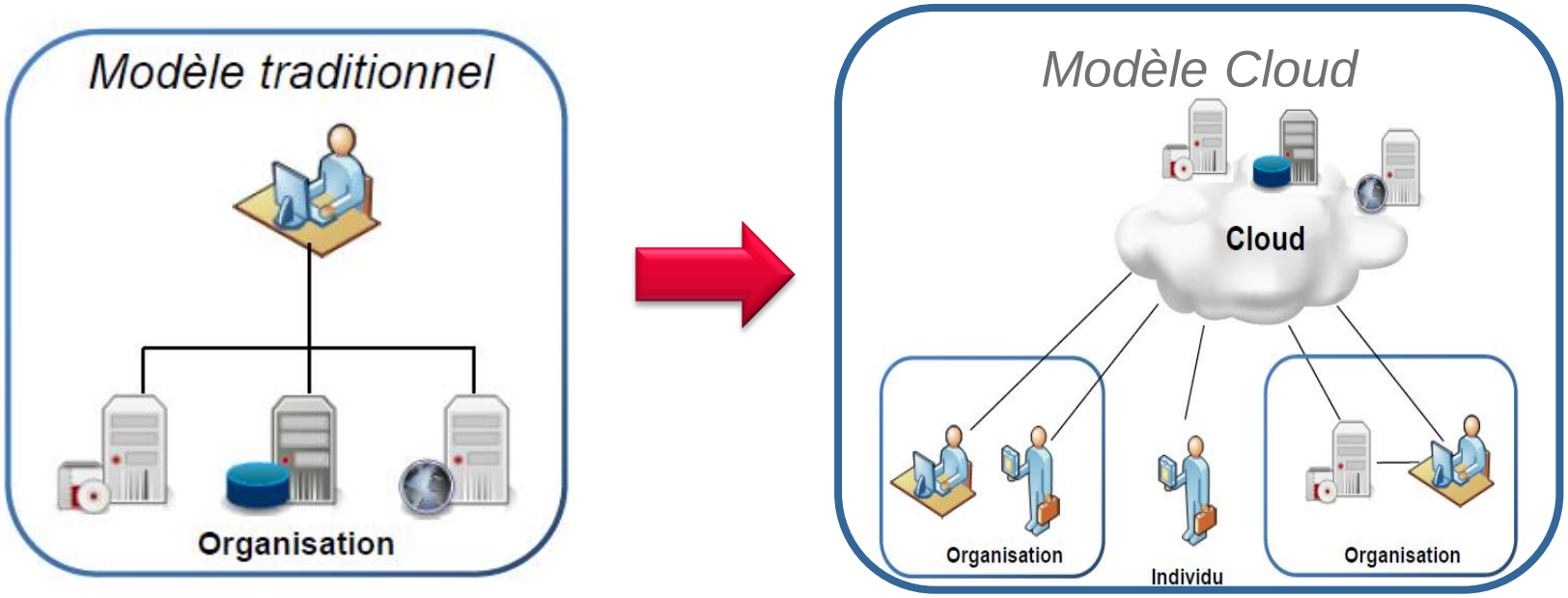
- Sujet vaste, à adapter en fonction des besoins sur les données

SOMMAIRE

CLOUD COMPUTING

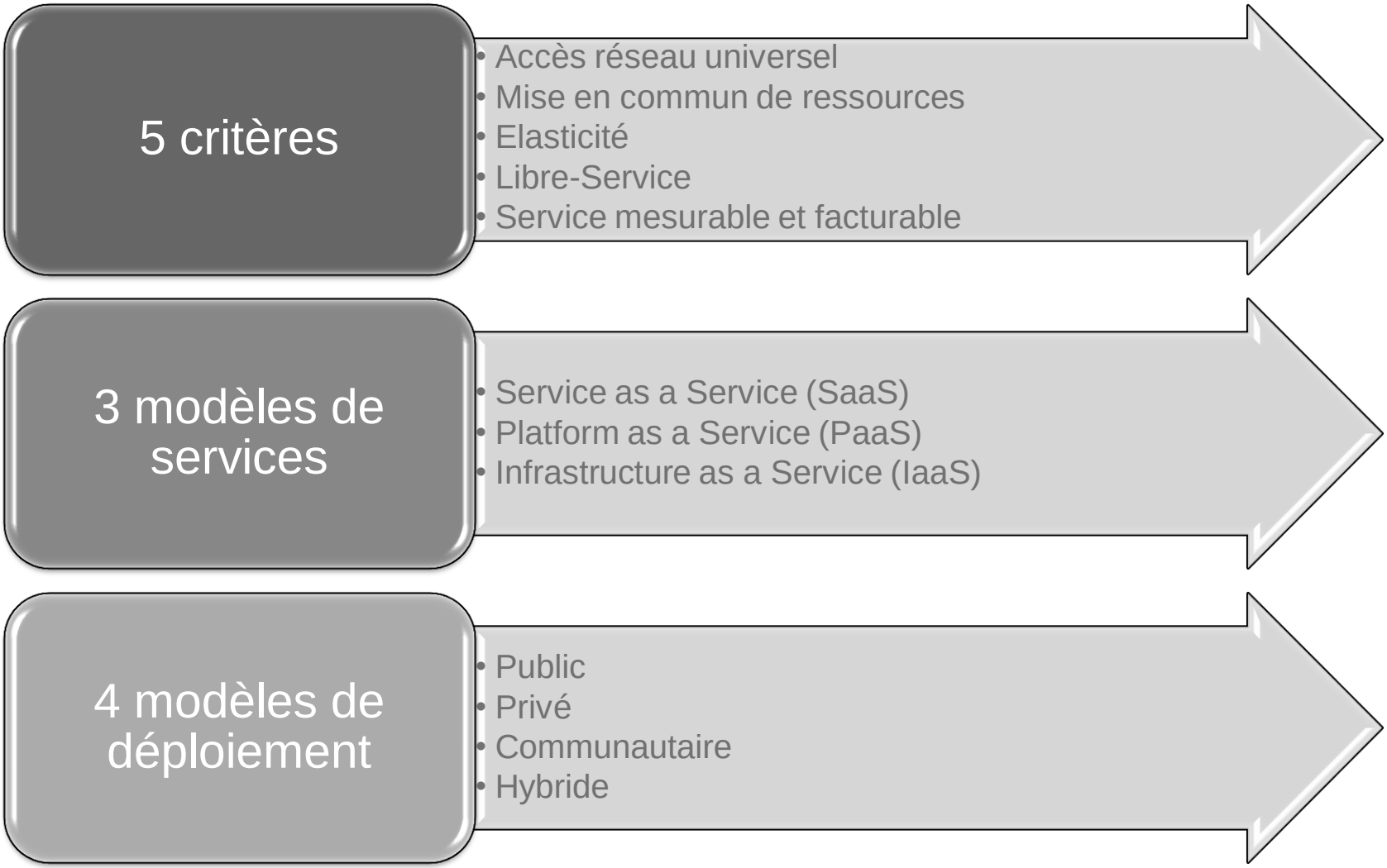
Définition

- Modèle traditionnel vs Modèle Cloud
  - Les données ne sont plus stockées dans les serveurs de l'entreprise
  - Accès aux données via un navigateur web
  - Emergence d'entreprises qui proposent les ressources de leurs infrastructures sous forme de services
- De nouvelles notions : l'évolutivité et l'élasticité
  - L'utilisateur peut faire varier les ressources demandées de manière dynamique
  - La facturation des ressources s'effectue par rapport à la consommation



CLOUD COMPUTING

Définition



CLOUD COMPUTING

Problématique

- Où se trouvent les données ? Quels traitements sur mes données ?
  - Réplication automatique des données dans le Cloud
  - Qui a accès ? (Patriot Act, etc.)
- Quelle règlementation s'applique à mes données ?
  - La CNIL interdit de transférer des données personnelles vers des pays qui n'offrent pas le niveau de protection adéquat.
- Qui sécurise les données (disponibilité, intégrité, confidentialité) ?
- Comment récupérer les données ?
  - en cas de disparition de mon hébergeur ?
  - En cas d'attaque DDoS sur l'hébergeur
- Et la Continuité d'Activité ?

Aux Etats Unis, ~80% des herbergeurs pensent que c'est au client de sécuriser ses données
En France, ~80% des clients, pensent que c'est à l'hébergeur de sécuriser ses données

CLOUD COMPUTING

Risques

- L'ENISA classe les risques liés au Cloud Computing en 4 catégories
  - organisationnels, techniques, légaux et non spécifiques au cloud

- Ci-dessous, les risques engendrant les plus forts impacts

Réf	Risques	Type de risque
R.2	Perte de la gouvernance	Organisationnel
R.3	Problème de non-conformité	Organisationnel
R.9	Problème d'isolation virtuelle	Technique
R.10	Employés malveillants côté fournisseur de Cloud	Technique
R.11	Compromission d'interface de gestion	Technique
R.14	Suppression non sécurisée des données	Technique
R.22	Perte de la localisation des données	Légal
R.26	Problèmes liés à la mauvaise gestion du réseau	Non spécifique cloud

Cloud Computing Security Risk Assessment : www.enisa.europa.eu

CLOUD COMPUTING

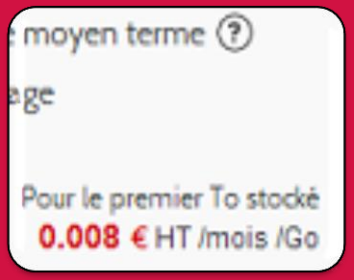
Conclusions

Réglementaire

- Evolution rapide des obligations réglementaires
- PCI-DSS, données de santé, etc.

Notion de bouquet de services

- Il est possible de sélectionner tout ou partie de son SI à déployer dans le Cloud



Axe économique

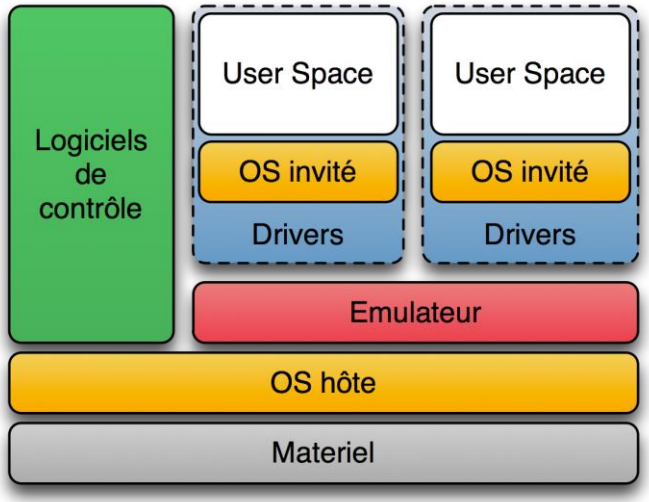
- La DSI se doit de fournir des solutions sinon, les utilisateurs ou les métiers vont les trouver… seuls
- Exemple d'OVH

SOMMAIRE

VIRTUALISATION

Définition

- Développé pour répondre au besoin d'extension des DSI
- Avant : les ordinateurs X86 ne pouvaient exécuter qu'un seul et unique système d'exploitation
  - avec parfois certains serveurs ne fonctionnant parfois qu'à 15%, voire 5% de leur capacité
- Architecture plus flexible, puissance adaptée au besoin
  - Redondance intersites en cas de sinistre rendu possible
- Réduction de la taille du parc informatique
- *Green IT*



La virtualisation permet de faire tourner plusieurs serveurs virtuels sur un ou plusieurs serveur physique

VIRTUALISATION

Problématique

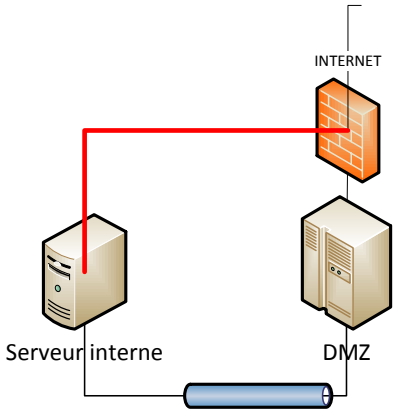
- Que se passe-t-il si un mainteneur/exploitant fait une erreur de manipulation ?
  - Que se passe-t-il si un mainteneur échange les câbles ?
  - Quelle manipulations peuvent être critiques ?
- Que se passe-t-il si ma machine physique tombe en panne ?
  - L'architecture repose malgré tout sur des composants physiques
  - L'accumulation de serveurs sur une machine physique augmente sa criticité
- Est-ce que mes serveurs sont bien cloisonnés ?
  - Disparition du cloisonnement physique
  - Protection de la supervision des machines virtuelles

VIRTUALISATION

Risques

- Une baie tombe en panne, plusieurs activités métiers sont immédiatement touchées

- Un utilisateur malveillant ou non parvient à prendre la main sur le superviseur



- Connexion accidentelle d'un serveur interne vers le web

VIRTUALISATION

Conclusion

« Matérialiser la virtualisation »

- Conserver une séparation physique des blocs fonctionnels

Limiter les erreurs

- Contrôler les accès
- Mise à jour régulière des OS

Analyser ses risques

- Impact de la perte du serveur host

QUESTION

CONTACT

Amaury COTHENET
Consultant Senior
Responsable de mission Résilience IDF

Mobile : +33 (0)6 58 35 51 42
E-mail : acothenet@LEXSI.com

LEXSI LYON

Bois des Côtes 1 - Bâtiment A
300 route Nationale 6
69760 LIMONEST
Tél. (+33) 8 20 02 55 20

LEXSI LILLE

Synergie Parc
4 rue Louis Broglie
59260 Lille-Lezennes
Tél. (+33) 3 59 57 05 16

LEXSI CANADA

3446-202 rue St-Denis
H2X 3L3 Montréal, Québec
Tél. +1 514 903 6560

LEXSI SINGAPORE

46 East Cost Road
Eastgate - #07-06
428766 Singapore
Tél. : +65 63 44 69 26

INNOVATIVE SECURITY

Pour vous aider à maîtriser vos risques

SIEGE SOCIAL

Tour Mercuriale Ponant
40 rue Jean Jaurès
93170 Bagnolet

www.lexsi.com