La sécurité de l'information dans les nuages

www.cnrs.fr

Journées JoSy – 19 et 20 mai 2014

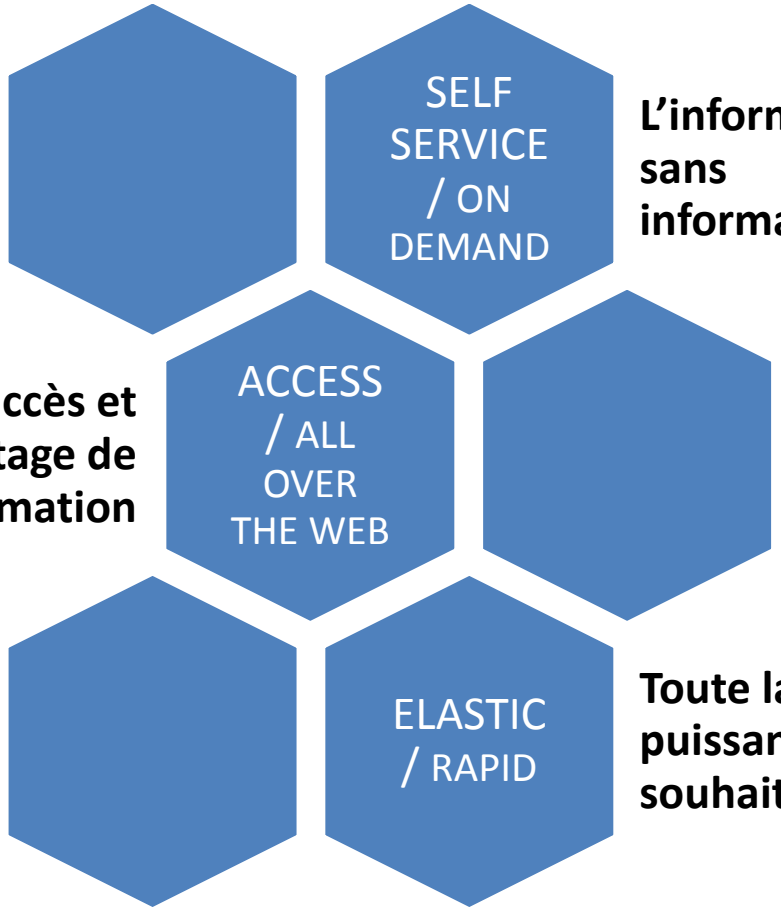
Louis Di Benedetto

RSSIC du CNRS

Une brève histoire de l'évolution ;-)

- Années 70 et 80 : les pionniers
  - Petit est le réseau, chacun garde son bien
- Années 90 et 00 : l'âge des utopies brisées
  - Le réseau est grand, le partage est (open) source de richesse, les pirates s'activent
- Années 10 : la guerre de l'information
  - Le réseau est tout, le contrôle du Cloud est la clé, les monopoles se consolident, qui sont les pirates ?

Le Cloud, Graal des années 2010 ?



L'information sans informatique

Comme je veux

« Open Admin »

Quand je veux
Où je veux
Avec qui je veux

Large accès et partage de l'information

« BYOD every where »

Toute la puissance que je souhaite

Autant que je veux

« Mutualisé »

9 problèmes dans le ciel (*)

- DATA BREACHES … *étanchéité*
- DATA LOSS … *réplication et sauvegarde*
- ACCOUNT / SERVICE HIJACKING … *authentification*
- INTERFACE / API INSECURE … *code sûr*
- DENY OF SERVICE … *résilience*
- MALICIOUS INSIDERS … *cloisonnement*
- ABUSE OF CLOUD SERVICES … *supervision*
- INSSUFICIENT DUE DILIGENCE … *vérifié*
- SHARED TECH. VULNERABILITIES … *sécurisé*

(*) The « Notorious Nine » (CSA 2013)

Un parapluie ou un ciré, fournisseur ou client ?

- Ai-je besoin de sécurité ?
  - Mon/son information est-elle ACID ?
  - Que peut-il m'arriver si ?
- Ai-je connaissance du risque ?
  - Le niveau du risque est-il élevé ?
- In fine je fais quoi ?
  - Gestion du risque ou pas, on continue ?

A qui faire confiance ?

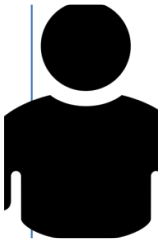
- Les fournisseurs
  - Gratuit vs. payant vs. souverain vs. académiques …
  - CGU et Livres blancs et la réalité …
  - Certifications par des tiers (à venir ?)
- Les organismes
  - A l'international, la bataille des normes
  - En France, l'ANSSI et le RGS (v2 ?)
- Et moi, et moi, et moi
  - Evaluation des risques ?

Quels leviers ?

HARD | SOFT | ARCHI | PROCESSUS

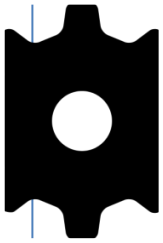
HUMAIN ?

ORGA



- POLITIQUE GENERALE
- EVAL RISQUES
- REPECT LOIS ET CONTRATS
- POLITIQUE INFORMATION
- AUDITS - CERTIFICATIONS

TECH

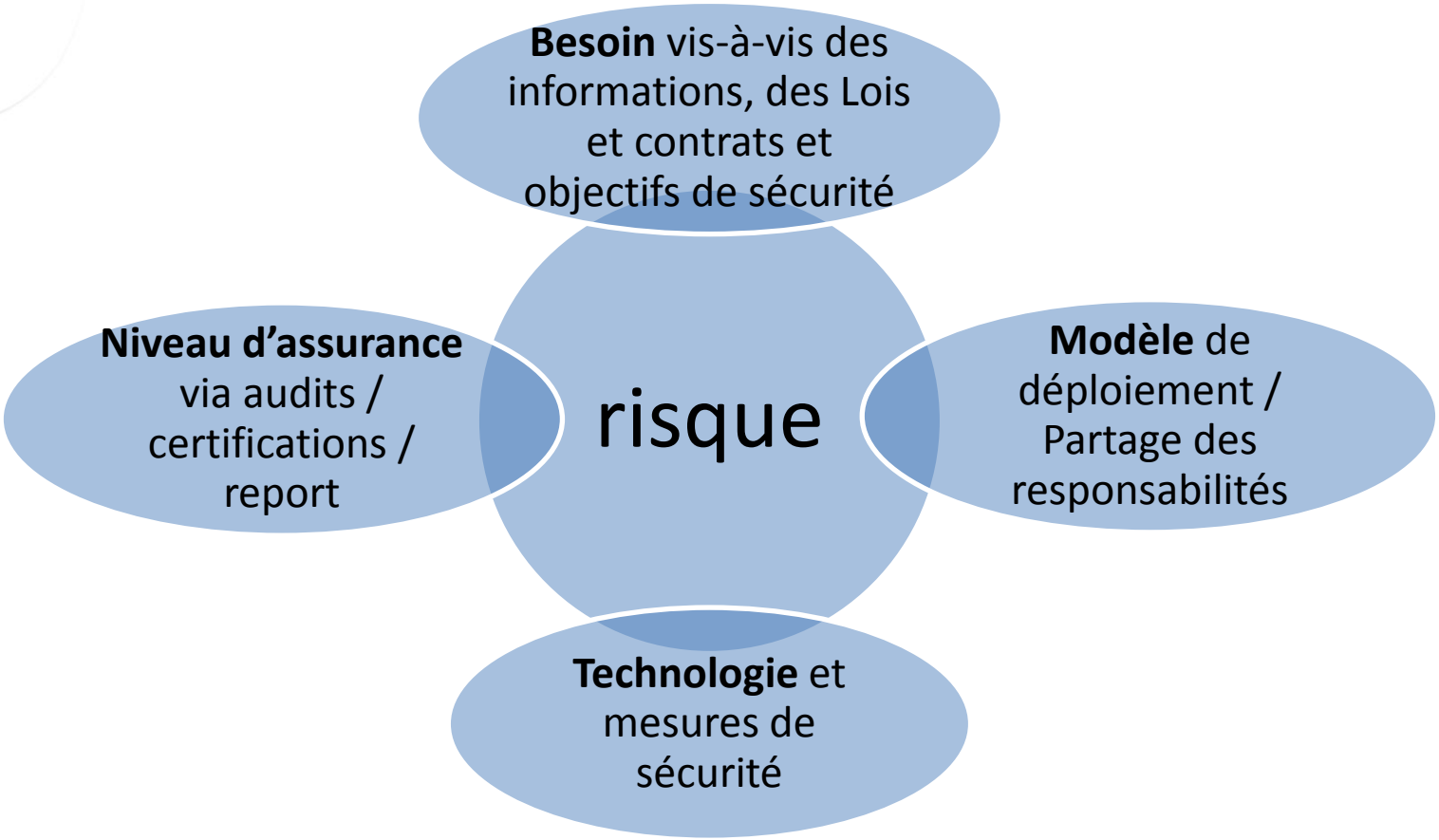


- INTEROPERABILITE
- SECURITE PHYSIQUE - PCA
- OPERATIONS DU DATA-CENTER
- GESTION DES INCIDENTS
- SECURITE DES APPLICATIONS
- CHIFFREMENT
- GESTION DES ID ET ACCES
- VIRTUALISATION
- SERVICES DE SECURITE

De la théorie à la pratique …

- OS et middleware vérifiés
- Développements sécurisés
- Chiffrement efficace
- Authentification renforcée
- Gestion des ressources maîtrisée
- Distribution des données fiable
- Outils d'administration robustes
- Supervision et défense active
- Contrats et SLA biens définis

La gestion du risque : un équilibre



Années 2020 …

- La suite est entre vos mains
  - What did you expect ?

- Questions ?