HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

ADIJ 20 janvier 2011

Sécurité du cloud computing

Frédéric Connes
<Frederic.Connes@hsc.fr>

Présentation d'HSC

- Cabinet de consultants en sécurité de l'information
  - Depuis 1989
  - 21 consultants
- Domaines d'activité
  - Sécurité technique : audits de sécurité, tests d'intrusion...
  - Sécurité organisationnelle : appréciation des risques, politiques...
  - Juridique : qualification OPQCM
  - Formations : inter, intra, e-learning
- Références clients
- Participation à de nombreux groupes de travail et associations

Critères de sécurité

- Confidentialité
- Intégrité
- Disponibilité

Avantages du cloud pour la sécurité

- Adaptation rapide aux besoins donc meilleure disponibilité
  - Augmentation/diminution de puissance à la volée
- Multiples instances physiques d'une même machine virtuelle
  - En cas de problème, possibilité de passer d'une instance à l'autre quasi instantanément
- Multiples copies des données
  - Potentiellement réparties sur plusieurs lieux géographiques
- Traitement au plus proche de l'utilisateur

Avantages du cloud pour la sécurité

- Déploiement de la sécurité
  - « Masters » de machines virtuelles durcies
  - Possibilité de revenir à une version antérieure opérationnelle
  - Possibilité de multiplier facilement les outils de sécurité
- Externalisation de la sécurité
  - IaaS : mutualisation de la sécurité physique/matérielle et du réseau
    - Disques en RAID, protection contre les attaques réseau...
  - SaaS : externalisation complète
- Analyse post-mortem, recherche de preuves
  - Possibilité de prendre une image du système sans l'arrêter

Risques du cloud

- Perte de maîtrise
  - Sur le matériel
    - Machines, électricité, climatisation, accès physique...
    - Toujours géré par le prestataire
  - Sur les logiciels
    - En SaaS et en partie en PaaS : aucun contrôle
    - En IaaS : risque d'utilisation de « masters » mal sécurisés voire compromis
  - Sur le réseau
    - Dépend de la connectivité du prestataire
    - Toujours géré par le prestataire
  - Risque que certaines mesures de sécurité soient impossibles à mettre en œuvre en raison des choix du prestataire
  - Risque de faux sentiment de sécurité (marketing du prestataire)

Risques du cloud

- Perte de contrôle sur les données
  - Généralement, le prestataire a potentiellement accès aux données
    - Sur les espaces de stockage
    - Administrateurs peuvent avoir les « clés » pour accéder aux comptes
    - Les accès du prestataire pourraient être compromis
  - Effacement de données
    - En fonctionnement normal ou en fin de contrat
    - Rien ne garantit que les données sont effectivement effacées
    - Sur tous les supports existants (serveurs, sauvegardes...)
    - Impossible d'utiliser des outils d'effacement réel
  - Certains prestataires peuvent toutefois se faire certifier (ex : SAS70)

Risques du cloud

- Machines virtuelles : risques liés à l'hyperviseur
  - Partage des ressources
    - Plusieurs machines virtuelles sur une même machine physique
  - Problèmes liés à l'isolation
    - Du stockage : données de plusieurs clients sur les mêmes disques
    - De la mémoire
    - Des processeurs
    - Du réseau
    - Mais les failles sont plus rares et les attaques plus complexes

Risques du cloud

- Risques liés à l'interface de gestion des services
  - Pour le cloud public
  - Compromission des données d'authentification
  - Conséquences
    - Suppression de serveurs ou de services
    - Actions en tant qu'administrateur
      - Par exemple si le changement de mot de passe est possible à partir de l'interface de gestion
    - Vol de données, transfert de services

Risques du cloud

- Risques pour l'obtention de certifications de sécurité
  - La migration dans le cloud peut invalider ou rendre impossible une certification (ex : PCI-DSS)
    - Le prestataire doit autoriser un audit de certification sur ses équipements
    - Il ne recherche pas nécessairement une telle certification
- Difficulté à organiser un test d'intrusion

- Réversibilité : risques pour la disponibilité
  - Impossibilité pratique de changer de fournisseur facilement
    - Ou de revenir à un hébergement interne
  - Absence de normes sur l'interopérabilité et la migration
  - Peut créer une dépendance forte

Questions