

La sécurité de l'information : une expertise au coeur de la stratégie de la Direction Conseil d'OPEN



Jean-Jacques BUREAU / OPEN Conseil
Senior Manager en charge de l'offre
Sécurité de l'information
Jean-jacques.bureau@open-groupe.com

Comment faire évoluer votre Datacenter en toute sécurité face à l'arrivée des offres de Cloud Computing ?

Afin de réduire les dépenses IT des centres de traitement des données (Datacenter) et d'offrir de nouveaux services à leurs clients, les DSI s'orientent vers la virtualisation des ressources et prennent en compte les offres récentes de Cloud Computing.

Le Cloud Computing assure la variabilité des ressources dans le temps, l'allocation dynamique et la disponibilité de celles-ci et s'appuie fortement sur la technologie de virtualisation. La conception de l'architecture virtuelle des Datacenter et son déploiement doivent impérativement intégrer les mesures de sécurité appropriées.

Concernant les Datacenter, la question primordiale est de savoir comment assurer la sécurité des données au travers des infrastructures virtuelles.

Les systèmes d'information, support du business, sont stratégiques pour les entreprises. Compte tenu du développement des communications sur des réseaux publics et du volume croissant des données à traiter voire à partager avec leurs partenaires, ces systèmes d'information possèdent une sensibilité élevée, et une vulnérabilité accrue pour les nouvelles architectures ouvertes, réparties et virtuelles. En conséquence, les données nécessitent d'être protégées en termes de confidentialité, intégrité et disponibilité.

La démarche permettant de sécuriser les Datacenter et les infrastructures virtuelles passe obligatoirement par la maîtrise des risques :

La première étape pour sélectionner les mesures de sécurité de façon efficace et en assurant la maîtrise des coûts, consiste à en apprécier les risques à l'aide d'une méthode de gestion des risques (par exemple, EBIOS 2010). Cette étape consiste à juger de l'importance des risques en les hiérarchisant selon les critères de gestion des risques retenus (disponibilité, intégrité, confidentialité...). De plus, il faut être conforme à la réglementation non seulement française mais aux réglementations européennes voire d'autres pays en fonction de la répartition des ressources et des données.

La deuxième étape de traitement des risques (refus, réduction, maintien ou transfert du risque) consiste notamment à identifier les objectifs de sécurité puis à étudier les mesures de sécurité.

Un Datacenter héberge, par construction, des ressources plus ou moins sensibles qui ont été identifiées lors de l'appréciation des risques ; il convient, dans un premier temps, de constituer des « zones logiques délimitées » permettant, en fonction de la catégorie de sensibilité, de séparer les parties les plus sensibles de celles qui le sont moins, dans le but de mieux contrôler les échanges entre ces différentes zones et d'adopter les mesures de sécurité en fonction de la sensibilité de la zone.

Quelles sont les trois formes de Cloud Computing existantes en entreprise :

- Le Cloud privé, interne à une organisation (grands comptes avec leurs filiales) ;
- Le Cloud externe, dédié à une organisation ;
- Le Cloud public ou mutualisé entre plusieurs clients.

Quelle démarche sécurité est utilisée en fonction de ces trois formes ?

Dans le premier cas, l'entreprise réalise l'étude des solutions de sécurité en adéquation avec l'évaluation des risques. Cette étude doit permettre d'assurer la sécurité des informations (au niveau confidentialité, intégrité, disponibilité...) et ceci, à travers des moyens de prévention des incidents (filtrage, authentification, contrôle d'accès...) et de détection (sonde de détection d'intrusion, supervision des moyens de sécurité, exploitation des journaux).

Associées à ces mesures techniques, il est nécessaire d'identifier les mesures non techniques et en particulier, clarifier les responsables des ressources et des biens sensibles.

Les mesures de contrôle d'accès aux données par des utilisateurs physiques ou par des applications en lien avec la problématique de gestion des identités et des accès (IAM) doivent absolument être accompagnées de « mécanismes d'étanchéité » des flux de données.

Les principales technologies d'étanchéité réseau sont les suivantes :

- réseau privé virtuel (ou VPN) : chiffrement, authentification et intégrité du trafic ;
- filtrage des flux en entrée/sortie des Datacenter, géré au niveau des pare-feux (ou FW) (adresse IP/protocole/port) ;
- zone démilitarisée (ou DMZ), cloisonnement

- de premier niveau, géré au niveau des pare-feux ;
- réseau local virtuel (ou VLAN), cloisonnement de deuxième niveau, géré au niveau des commutateurs (adresse MAC) ;
- Private VLAN, cloisonnement de troisième niveau et géré au niveau des commutateurs (ports physiques) ;
- contrôleur d'accès au réseau (ou NAC) qui permet notamment le contrôle de la connexion des postes au réseau ;
- système de détection d'intrusion (ou IDS) qui détecte les anomalies sur la base de signatures ou d'analyse comportementale ainsi que les attaques au niveau applicatif ;
- système de prévention d'intrusion (ou IPS) qui possède les mêmes fonctionnalités que les IDS mais avec la possibilité de réaction automatique face aux intrusions et blocage des attaques en temps réel ;
- corrélation de journaux de sécurité qui facilite la gestion des alertes et apporte une vision globale des événements de sécurité.

Dans les second et troisième cas, lorsque le Cloud Computing est géré par un prestataire externe, l'entreprise conserve la responsabilité de ses données et notamment celles des données de ses clients. Le prestataire garantit alors le niveau de sécurité des données en termes de disponibilité, intégrité et confidentialité.

En particulier, l'entreprise s'assure en amont de la contractualisation que le prestataire respectera toutes les exigences de sécurité en adéquation avec le niveau de sécurité requis, et que les mesures de sécurité seront correctement mises en œuvre, notamment :

- mise à disposition d'une politique sécurité ;
- conformité à la réglementation ;
- sécurisation physique des zones concernées ;
- sécurisation de l'exploitation dont le cloisonnement entre clients en cas de mutualisation ;
- sécurisation des transferts de données ;
- réplication des données et mise à jour des données répliquées ;
- mise en œuvre des mesures d'étanchéité réseau ;
- contrôle d'accès.

La mise en œuvre des mesures de sécurité n'est pas si complexe et peut contribuer à la maîtrise des coûts si l'on utilise une démarche pragmatique basée sur la maîtrise des risques.

L'évolution progressive des Datacenter avec le déploiement de solutions de Cloud Computing peut ainsi s'appréhender tout en assurant le niveau de sécurité requis.

Avec près de 3 700 collaborateurs en France et à l'international, OPEN se positionne comme un acteur de la Performance des Directions Informatiques des grandes entreprises. Cotée en bourse, OPEN figure parmi les 10 premières SSII françaises (CA 2009 : 290 M€) et exerce ses trois métiers - Conseil, Ingénierie Applicative et Infrastructures Services - en conjuguant professionnalisme, innovation et proximité à travers une organisation intégrée au plus près des centres de décision et de production de ses clients.

OPEN a pour ambition de consolider sa position parmi les toutes premières SSII en France par notamment l'évolution de son modèle en s'appuyant sur ces 5 valeurs : Pertinence, Audace, Ethique & Responsabilité, Passion et Engagement.

La Direction Conseil d'OPEN accompagne les directions générales et informatiques de grands groupes et de PME/PMI. Sa valeur ajoutée repose sur des offres continuellement adaptées et actualisées pour accompagner les évolutions de ses clients dès lors qu'elles concernent les métiers, les organisations et processus, les systèmes d'information et la sécurité de l'information.