C'est probablement l'une des idées reçues les plus répandues : le fait de migrer des infrastructures ou des applications dans le cloud permettrait aux entreprises de s'affranchir de la nécessité de disposer d'un plan de reprise d'activités (PRA). En réalité, le cloud ne dispense absolument pas de se préoccuper de plan de reprise d'activités. Les problématiques de performance, de disponibilité (24/7) et de sécurité, sans oublier l'innovation restent au cœur des enjeux des DSI :

Ainsi, ce qui était sécurisé dans un « datacenter » doit aussi l'être dans le cloud, met en garde Didier Lavoine Directeur Technique, Développement et Innovation de l'entreprise de services Digora, qui nous livre son analyse.

Ensuite, il est risqué de s'en remettre à la seule disponibilité offerte, en standard, par le cloud, même avec des engagements de qualité de services. En effet, des ruptures de services plus ou moins prolongées affectent inévitablement, et de manière significative, l'activité des entreprises, avec des conséquences directes (perte de chiffre d'affaires, insatisfaction des clients, désorganisation logistique...) ou indirectes (atteinte à l'image de marque, responsabilités contractuelles...).

Une nouvelle approche du PRA :

- Le cloud ne répond pas de manière native à tous les risques, en particulier aux principales vulnérabilités dont tout système d'information peut être victime un jour ou l'autre, et de manière aléatoire, par exemple la corruption de données, la défaillance d'un opérateur de télécommunications (non couverte dans les contrats cloud), d'un composant ou d'un serveur, ou encore l'erreur humaine.

- La philosophie traditionnelle d'un PRA repose généralement sur l'existence de deux « datacenters », avec une réplication des données entre ceux-ci, de manière plus ou moins synchrone, en fonction des besoins de sécurité. Mais cette approche, si elle présente un niveau de sécurité suffisant, a néanmoins un coût très élevé, d'autant que la probabilité de survenance des risques peut être relativement faible. Elle est donc de plus en plus difficile à justifier lorsque l'on met en parallèle le coût de la protection et les pertes réelles subies (en principe nulles si la sécurité est bien assurée...). À supposer, bien sûr, que le PRA soit correctement et régulièrement testé... Avec le cloud, cette architecture reposant sur deux « datacenters » doit être reproduite en tenant compte des implantations des « nuages ».

- Comment « justifier la duplication » de ce qui fonctionne bien car cela a un coût certain. Le premier principe consiste à identifier les ressources nécessaires, de manière à bien les dimensionner par rapport aux trois besoins essentiels de sécurité : la disponibilité, l'intégrité et

la confidentialité. Les différents métiers dans l'entreprise n'ont pas les mêmes besoins et un PRA doit les prendre en compte.

Incontournable « Business Impact Analysis » :

- La seconde phase s'attache à identifier les risques, en intégrant une approche de BIA (Business Impact Analysis). Elle a pour objectif d'analyser de manière détaillée les processus métiers et leur impact sur le fonctionnement de l'entreprise. On analyse ainsi les impacts susceptibles d'affecter la continuité des activités de l'entreprise, les risques plausibles et concrets, avec leur degré de gravité, ainsi que la quantification des pertes.

- Ensuite, l'architecture du PRA est construite en fonction de cette analyse de risques. Les spécificités du PRA seront ainsi fonction de la nature des risques et de leur probabilité d'occurrence. Il convient de déterminer également les PDMA (Pertes de Données Maximales Admissibles) et les DMIA (Durées Maximales d'Interruption Admissibles), une réplication synchrone n'étant pas toujours possible (elle dépend de la distance entre deux sites), voire souhaitable, selon les exigences métiers. Ainsi, l'architecture d'un PRA dans le cloud public sera basée sur deux clouds distants et deux opérateurs, avec un principe de réplication via les deux opérateurs.

- Quel que soit l'environnement, l'une des difficultés est de gérer le risque humain. Est-ce une mission impossible pour les DSI et les RSSI ? Non, car cet aspect peut être efficacement géré grâce aux fournisseurs de services managés. Ils peuvent en effet réduire considérablement l'erreur humaine, et en mode agile, avec l'expertise des prestataires en matière de supervision, d'administration, d'automatisation des actions ou de SOC (Security Operations Center). Des expertises qu'il est de plus en plus difficile de mettre en œuvre dans les entreprises sans un accompagnement adapté et agile...

Source : ITRNews