Intitulé de l'épreuve : Note de Synthèse

Nombre de copies :

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Introduction

L'informatique en nuage (Cloud computing) doit permettre l'accélération de la transformation numérique des administrations. Le gouvernement pousse celles-ci vers cette technologie avec la doctrine "Cloud au centre"

Nous allons tout d'abord voir ce qu'est le "cloud" et quelles en sont les offres. Nous verrons ensuite qu'une telle migration n'est pas sans risque et nécessite de prendre des précautions en amont.

I le cloud computing et ses différentes offres

le cloud computing est "un mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire" comme le définit le Journal officiel du 6 juin 2010. Il s'appuie sur des nouvelles technologies : virtualisation et calculs distribués.

3 solutions techniques sont généralement proposées, l'infrastructure as a service" (IaaS), la "plateforme as a service" (PaaS) et le "Software as a Service (SaaS)

N° ... 1 ...

la première solution (IaaS) offre une liberté de choix technologiques tandis que les 2 autres proposent des outils clé en main et s'adressent à des développeurs pour le PaaS et aux utilisateurs pour le SaaS.

Il existe 3 offres pour mettre en œuvre ces solutions : le "cloud interne", le cloud commercial de confiance et le cloud commercial générique. L'état a mis à la disposition des administrations 2 clouds internes qui ne sont donc pas gérés par de société privées. Cette solution offre un niveau de sécurité élevé mais propose peu de flexibilité au niveau des besoins. le cloud commercial de confiance est plus adaptable tout en offrant un bon niveau de sécurité des données puisque celles-ci sont hébergés dans l'Union Européenne. le cloud commercial générique est l'offre qui propose le catalogue le plus important. En revanche le niveau de sécurité des données est faible. celles-ci peuvent être hébergées hors UE.

Cette nouvelle architecture comporte néanmoins des risques pour lesquels il est nécessaire de prendre des précautions.

II Risques et précautions à prendre

1) les risques

Lorsque les données sont stockées dans le cloud elles s'éloignent physiquement de nos locaux et donc une partie de la protection est déléguée à un tiers. Il est donc important de mesurer ces risques en amont.

[redacted]

Les données peuvent être perdues par l'hébergeur par négligence. C'est le cas de la société OVH qui a subi un incendie dans un de ses data centers. De nombreux clients (collectivités, entreprises, administrations) ont été durement touchés car en plus d'avoir perdu des données, leur activité a dû être arrêtée pendant 1 de jours.

De plus, les données dans les data centers sont plus difficiles à protéger des attaques de cybercriminels.

Enfin si les données sont hébergées hors de France ou pire, hors UE, elles peuvent subir des contraintes juridiques et donc ne plus être protégées. C'est ainsi que les grands acteurs du marché Amazon, Google sont susceptibles de fournir au gouvernement américain certaines des données qu'ils hébergent (Cloud Act).

Face à ces risques, il convient de prendre des précautions

2) <u>Précautions</u>

Le gouvernement et l'ANSSI (Agence Nationale de Sécurité des systèmes d'information) sensibilisent les administrations et donnent des recommandations en les dirigeant vers les offres les plus sécurisées tel le Cloud interne et le cloud commercial de confiance. (l'ANSSI propose un cahier des charges pour la sélection des prestataires)

Le cloud interne paraît la solution la mieux adaptée à notre administration : les données sont hébergées par le gouvernement et donc soumis à la législation française. Ce type de cloud a l'avantage aussi d'être connecté à notre

N°

... / ...

interministériel
réseau VPN sécurisé RIE. Avec ce choix, on éviterait le risque d'un hébergeur low-cost qui fait des économies sur la sécurité des données comme OVH.
Concernant la menace des attaques cybercriminelles là aussi, ce type de cloud semble le mieux adapté car nos partenaires en charge de l'hébergement des données sont au fait face à ce genre de risques.

Je propose aussi de retenir la solution de l'IaaS, ce qui permettra à nos équipes de garder leur liberté de technologie.

Il nous faudra aussi adapter notre Plan de Relance d'Activités et le consolider. C'est très important. Nous ne sommes pas à l'abri d'incidents imprévus. Nous devons le continuité du service public.

Conclusion :

Le cloud va permettre à notre Direction de se moderniser encore en proposant des outils innovants à nos équipes. Ces outils vont ensuite permettre en bout de chaîne de proposer aux utilisateurs des applications et des moyens de travailler toujours plus proches de leurs besoins.
Pour répondre aux contraintes de sécurité des données de notre ministère, je préconise que notre ministère s'oriente vers des "Infrastructures as a Service" dans un des clouds internes de l'Etat.

N°
... /...