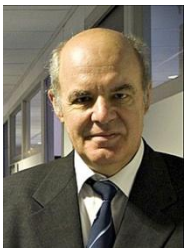
LA TÊTE DANS LES NUAGES



Par Gérard Peliks
Expert sécurité
Président de l'atelier Sécurité de Forum ATENA

Cet article est paru dans le numéro 103 de Signaux, la revue d'ISEP Alumni, « Le nouvel usage des TIC » daté du 18 mai 2012

Il est reproduit avec l'aimable autorisation d'ISEP Alumni.

Le cloud computing est un sujet d'actualité. Les années 2010 seront celles de la mobilité, offerte notamment pas le cloud computing. A vous les compétences métiers… au cloud la gestion de votre Information…

Mais le cloud est-il la réponse à tous vos problèmes ou le début de gros problèmes ?

LES BASES DU CLOUD COMPUTING

LA GENÈSE DU CLOUD COMPUTING

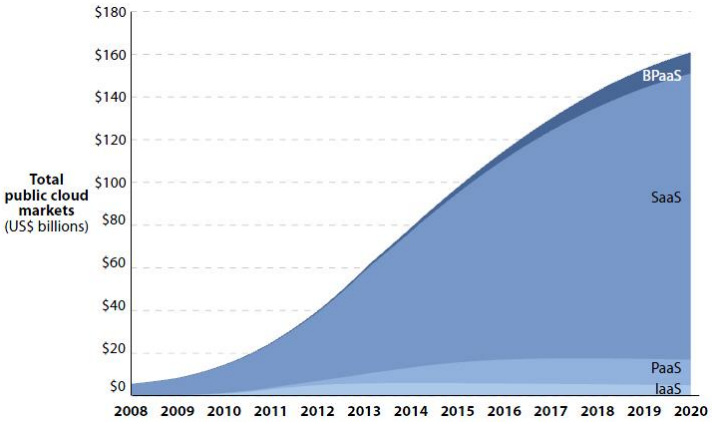
Si on remonte aux années 1970, il existait des gros ordinateurs « mainframes » auxquels les utilisateurs présentaient leurs travaux en « batch », chacun son tour.

C'est dans les années 1980 que l'informatique a commencé à s'individualiser, avec les premiers ordinateurs personnels ou avec des services de temps partagé sur de gros ordinateurs sur un modèle client-serveur.

Les années 1990 ont vu le développement de la « toile », le World Wide Web, qui s'est rapidement présentée comme un vaste espace de stockage et de partage de données.

Les années 2000 furent celles des ASP (Application Service Provider).

Enfin les années 2010 sont celles du « cloud » ou informatique en nuage, dont l'envolée est plus qu'un épiphénomène.



Marché du cloud computing (Forrester Research Inc.)

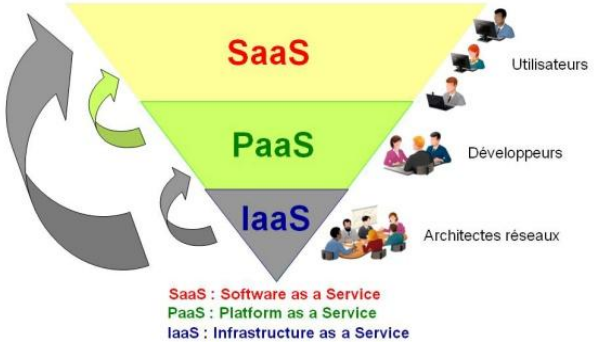
MAIS QU'EST-CE QUE LE CLOUD COMPUTING ?

A la base, on trouve Internet et les multiples serveurs qui lui sont raccordés. La capacité offerte par ces serveurs est gigantesque, tant en volume de stockage qu'en puissance de calcul. L'idée est simple : plutôt que stocker ses fichiers sur notre ordinateur, allons les stocker sur un serveur. Plutôt que d'utiliser des logiciels résidents sur notre ordinateur, allons utiliser les logiciels présents sur un serveur.

L'utilisateur n'a plus besoin que d'un ordinateur de faible puissance, à la limite un smartphone, pour utiliser la puissance informatique des machines du cloud.

En termes de cloud computing, on distingue plusieurs modèles de services :

- **Iaas** (Infrastructure as a Service) est la mise à disposition de matériel informatique dans le cloud, évitant aux utilisateurs des investissements lourds en matériel
- **Paas** (Platform as a Service) est la mise à disposition de matériel informatique et de logiciels dans le cloud, soit tout ce qui est nécessaire au développement d'applications informatiques
- **Saas** (Software as a Service) est la mise à disposition de logiciels, évitant l'achat de licences et de mises à jour d'un parc d'ordinateurs privés.
- **BPaaS** (Business Process as a Service) met à disposition des solutions CRM de gestion de la relation client des entreprises.



Du côté de l'infrastructure, les avantages sont multiples :

- utilisation optimale des ressources d'un parc de machines par répartition des machines virtuelles sur les machines physiques,
- économie sur le matériel par mutualisation,
- allocation dynamique de la puissance de calcul en fonction des besoins.

Le cloud computing aurait aussi des conséquences sur l'environnement. Selon une étude réalisée par le cabinet d'analyse Verdantix et financée par AT&T, les entreprises françaises qui opteraient pour le cloud computing verraient leur facture énergétique baisser de 830 millions d'euros et engendrer une réduction annuelle des émissions de carbone équivalentes à celles de 630.000 voitures… Mais selon Greenpeace, les émissions de gaz à effet de serre issus des centres de traitement de données qui utilisent près de 2% de l'électricité mondiale qui proviennent en majorité de centrales au charbon devraient tripler d'ici 2020…

Du point de vue de l'utilisateur, les avantages sont aussi multiples :

- services obtenus à la demande,
- accès de n'importe où, n'importe quand,
- ressources mutualisées,

- élasticité,
- paiement à la consommation.

QUI CONTRÔLE QUOI ?

Si l'utilisateur maîtrise un certain nombre de facteurs dans la gestion de son Information avec l'IaaS, il en maîtrise beaucoup moins avec le PaaS et presque rien avec le SaaS, juste les informations qu'il y injecte et celles qui en ressortent. Nous laissons de côté le BPaaS, que l'on assimilera au SaaS.

Il existe d'autre part quatre modèles de déploiement :

- le cloud privé où l'entreprise est la seule utilisatrice,
- le cloud mutualisé utilisé par plusieurs entités mais en nombre limité et donc connu au moins par le prestataire du cloud,
- le cloud public pouvant être utilisé par tout le monde et ouvert sur l'Internet,
- le cloud mixte qui se situe entre le cloud mutualisé et le cloud public.

LES RISQUES

Le cloud privé, par sa nature, ne présente pas de risque particulier, l'utilisateur restant maître de la chaîne de traitement. On peut considérer qu'il en est de même avec le cloud mutualisé.

Les ennuis commencent avec le cloud public ou mixte où l'utilisateur, lié à son fournisseur, pourra se heurter à des failles de sécurité, tout d'abord sur la gestion des données elles-mêmes :

- compartimentation imparfaite des données de différents utilisateurs,
- mauvaise protection de l'information,
- suppression des données non sécurisée ou incomplète.

Ajoutons à cela, les risques humains :

- compromission de l'interface de management,
- employé du prestataire de cloud peu scrupuleux.

Enfin, il ne faut pas perdre de vue que de nombreux clouds sont hébergés dans des pays soumis à une politique plus laxiste que la nôtre en matière de protection de l'information et que le client reste responsable de ses données qui, si elles sont à caractère personnel, ne doivent pas quitter l'Europe, voire le territoire national dans certains cas.

LES HACKERS

Le cloud constitue une pièce de choix pour les hackers qui pourront y faire un marché fructueux : mots de passe, coordonnées bancaires, comptabilité des entreprises… et j'en passe !

De plus le cloud offre lui-même ses armes au hacker en lui mettant à disposition une capacité de calcul quasi illimitée. En ouvrant une connexion sur des centaines d'ordinateurs en parallèle, le hacker peut « casser » en quelques heures un mot de passe qui autrefois aurait résisté à plusieurs années de traitement.

CLOUD ET SÉCURITÉ

FAUT-IL CHIFFRER TOUT CE QU'ON MET DANS LE CLOUD ?

Il est difficile de répondre par oui ou par non à cette intéressante question quand on appréhende la complexité du cloud et celle du chiffrement.

Il semblera à un public, non expert en technologie du cloud, mais néanmoins conscient de l'obligation de sécuriser son Information, qu'une réponse affirmative aille de soi. Dans la mesure où l'utilisateur n'a plus la souveraineté sur le stockage et le traitement de son Information, oui, de toute évidence il faut chiffrer tout ce qu'on met dans le cloud. Alors, pourquoi n'est-ce pas si simple de répondre à cette question ? Et si on le souhaitait, est-ce possible de tout chiffrer ?

En associant chacun des modèles de service à chacun des modèles de déploiement on obtient un certain nombre de combinaisons qui mériteraient pour chacune, une réponse spécifique. L'exercice serait intéressant mais un peu long.

Laissons de côté le cloud privé qui n'apporte ni n'enlève rien à ce qui existait déjà chez l'utilisateur et ne présente pas de risque supplémentaire.

La question commence à se poser avec le cloud mutualisé puisque l'entreprise n'est plus toute seule sur les serveurs où est contenue son information. En principe, en tout cas sur le contrat qui définit les rôles et les prestations et lie le prestataire du cloud à son client, l'étanchéité est garantie entre tous les clients. Mais nul n'est à l'abri d'une vulnérabilité cachée, par exemple dans les couches basses du système de virtualisation, qui rendrait le système poreux. Alors là oui, il est préférable de chiffrer les informations qui doivent rester confidentielles ainsi que les données à caractère personnel protégées par des lois et des réglementations.

A la question « *peut-on mettre des informations confidentielles dans le cloud ?* » on peut répondre que tout dépend du niveau de confidentialité attendu pour ces informations. Si ce sont des données classifiées Défense qui ne doivent en aucun cas être mises dans un réseau qui pourrait être ouvert à ceux non habilités à en prendre connaissance, il ne peut à plus forte raison être question qu'elles soient hébergées et traitées dans un cloud, que ces données soient chiffrées ou en clair.

Les données dites à caractère personnel sont soumises à des réglementations particulières, nationales ou régionales[1]. Par exemple de telles données utilisées dans un pays européen, ne doivent pas quitter le territoire européen, sauf exceptions ou permissions, qu'elles soient chiffrées ou qu'elles soient en clair. Comme le cloud computing ne connait pas vraiment de frontières, sauf précautions et assurances spéciales prises par les prestataires de cloud, le cyber espace peut représenter une menace pour les données, et entrainer des complications juridiques pour ceux qui les gèrent. Le chiffrement, dans ce cas là, n'apporte pas une solution miracle.

Les autres catégories : cloud mixte, et cloud public d'autant plus, nécessitent soit de chiffrer soit de ne pas mettre d'informations confidentielles ou de données à caractère personnel dans le cloud. Mais cela entraine des problèmes de gestion de clés que nous allons également aborder.

LE CHIFFREMENT POUR ASSURER LA CONFIDENTIALITÉ

Venons en maintenant à l'aspect chiffrement. Sans entrer dans le détail, pour chiffrer une information, il faut un algorithme et une clé, et il faut aussi une autre clé (chiffrement asymétrique) ou la même (chiffrement symétrique) pour déchiffrer. Le plus souvent on utilise le chiffrement symétrique pour chiffrer et déchiffrer et le chiffrement asymétrique pour échanger les clés de chiffrement symétrique. Dans le cloud, si on chiffre, la question est de savoir qui doit gérer les clés.

Si l'utilisateur gère lui-même ses clés, seul celui qui a les clés pourra manipuler l'information confiée au cloud, ce qui semble être une bonne solution. Mais il ne faut pas cacher que la gestion des clés de chiffrement, la génération d'aléas et de clés secrètes symétriques, le renouvellement de ces clés, la gestion des clés privées asymétriques et des certificats (problèmes des PKI – Infrastructures de clés publiques) ne sont pas des tâches particulièrement simples. Alors, puisque le cloud est là pour simplifier la tâche de l'utilisateur en l'affranchissant de la technique, pourquoi ne pas confier également la gestion des clés à un cloud ?

Le problème est alors que si vos informations chiffrées sont dans un cloud avec le moyen de les déchiffrer, il faut que vous gardiez une sacrée confiance envers le prestataire. Vous devrez aussi vous persuader que parmi les autres clients du cloud, certains n'en profiteront pas pour utiliser les clés et déchiffrer vos données. Il est sûr que ce n'est pas une chose triviale que de déchiffrer les données des autres avec les clés qu'on a récupérées. De plus cela suppose une certaine porosité, dont on a déjà parlé, et qui n'est pas le cas naturel d'un cloud. Mais où s'arrête la méfiance lorsque la sécurité est en jeu ?

Une idée est de confier ses données chiffrées à un prestataire de cloud et la gestion des clés de chiffrement à un prestataire d'un autre cloud. Ainsi l'utilisateur est débarrassé du souci de la gestion de ses clés. N'est-ce pas précisément la fonctionnalité attendue d'un cloud : simplifier la vie, économiser les ressources financières et humaines, occulter les difficultés techniques, en un mot laisser gérer les affaires des clients sans les obliger à entrer dans des détails qui ne sont pas dans leur corps de métier ? C'est je pense une bonne idée et l'avenir apportera de tels montages avec les **métaclouds**. Un nuage de nuages pour que ciel reste dégagé de toutes difficultés au dessus des utilisateurs ! Mais les métaclouds aujourd'hui sont plutôt du domaine des recherches avancées dans les laboratoires et n'ont pas encore, à ma connaissance, de déclinaison pratique.

Donc, pour répondre à la question : « *Faut-il chiffrer tout ce qu'on met dans un cloud ?* », la réponse que je ferai à ce stade est « *Non pas tout ce qu'on y met, mais il faut, au moins dans un cloud non privé, chiffrer l'information confidentielle pour assurer sa confidentialité* ». Mais il faut aussi gérer les clés de chiffrement alors, soit on prend le risque de confier cette gestion à un prestataire de cloud, soit on le fait soi-même.

Mais le chiffrement peut assurer bien plus que la seule confidentialité.

---

[1] *L'article 68 de la loi du 6 janvier 1978, modifiée le 6 août 2004, dispose, conformément à l'article 25 de la directive européenne du 25 octobre 1995, que le transfert de données à caractère personnel (information se rattachant à une personne physique et permettant l'identification même indirecte de celle-ci) hors de l'Union Européenne n'est licite/possible que si le pays destinataire des données présente un niveau de protection suffisant ou équivalent au droit communautaire*

LA SIGNATURE POUR ASSURER L'INTÉGRITÉ ET L'AUTHENTICITÉ

Quand vous confiez vos données à un cloud, vous demandez que seuls les utilisateurs autorisés puissent en prendre connaissance.

La confidentialité, mise en œuvre par le chiffrement, remplit cette demande. Mais rien ne prouve que les données, même chiffrées, n'ont pas été modifiées. Justement, le chiffrement peut également assurer cette fonction de vérification de l'intégrité et aussi celle de la vérification de l'authenticité des données confiées au cloud. L'authenticité est la preuve que les données ou les programmes de traitement de ces données créés par une personne ou une entreprise, sont bien celles de cette personne ou de cette entreprise.

Le mécanisme de la signature électronique, basé sur le calcul d'empreintes et sur les mécanismes de chiffrement, permet de garantir l'intégrité et l'authenticité des informations et des programmes qui les traitent. J'apporterai une réponse un peu à côté de la question posée : « *Oui, il faut tout signer ce qu'on met dans le cloud* ».

Bien sûr, la signature électronique apporte aussi son lot de difficultés techniques : gestion des clés de chiffrement, génération des certificats électroniques, signature par une autorité de confiance, mais, à mon sens, plus on perd la gouvernance de ses informations et de leurs traitements, plus on a besoin de prouver l'intégrité et l'authenticité de ce qu'on récupère venant du cloud.

LE VPN POUR SÉCURISER LES ÉCHANGES

Jusque là, nous avons évoqué seulement le chiffrement des informations stockées et manipulées dans le cloud. Il est une question qu'il ne faut surtout pas oublier : « *Faut-il chiffrer tous les canaux d'échanges des informations entre le cloud et l'utilisateur ?* »

Quel que soit le cloud, du privé ou public, quel que soit le modèle SaaS, PaaS ou IaaS, la réponse est « oui ». Bien entendu il faut utiliser le chiffrement pour assurer la confidentialité, l'intégrité et l'authenticité (et également la non répudiation) de ce qui transite entre le prestataire de cloud et son client.

Pour ce faire, la technique du VPN (Virtual Private Network, ou Réseau Privé Virtuel) apporte une bonne solution. Parmi les VPN possibles, si l'utilisateur accède à l'information par son navigateur, le protocole SSL (Secure Socket Layer) est de toute évidence la solution qui s'impose. Aucune connaissance technique n'est nécessaire pour utiliser le VPN SSL. Tout navigateur est un client SSL prêt à l'emploi sans qu'il soit nécessaire pour l'utilisateur d'en avoir conscience. Simplement l'adresse Web, par laquelle vous accédez à vos informations, commence par *https* et non par *http* et il y a un cadenas fermé sur lequel, en cliquant deux fois, vous obtenez, entre autres renseignements, l'autorité de confiance qui a signé le certificat électronique du serveur par lequel vous accédez à vos informations.

Avec cela, vous êtes quasi certains que les informations qui transitent entre vous et le prestataire de cloud, ne seront ni lues, ni modifiées durant le transfert. Donc, pour répondre à la question posée : « *Oui, évidemment, il faut utiliser un VPN pour toutes les transactions entre le cloud et vous* ».

Le VPN SSL offre à l'utilisateur l'assurance qu'il s'adresse bien à son prestataire de cloud. Il faut aussi que le cloud s'assure, de son côté, de l'identité/authenticité de l'utilisateur avant de lui accorder les ressources, et là encore, en général, cela fait appel à des fonctions de chiffrement mais qui sont en dehors du sujet traité et on peut espérer que tout prestataire de cloud met en jeu un mécanisme d'identification/authentification rigoureux, sinon d'autres que vous pourraient accéder à vos données.

DEUX CAS PARTICULIERS

Pour ne rien omettre, il faut citer des cas où, bien que le chiffrement soit indispensable, il n'est pas possible de l'utiliser.

Dans certains pays, et on pense souvent immédiatement à la Chine, chiffrer est un délit. Rappelons à cet effet qu'il n'a pas toujours été facile d'être autorisé à chiffrer, en France, avec des clés de longueur suffisante, mais cette histoire appartient au passé. En Chine, et dans quelques autres pays, l'interdiction est par contre très actuelle. Si vous travaillez dans une filiale française d'une entreprise basée à Hong Kong et dont les informations sont dans un cloud hébergé principalement à Pékin, ne suivez pas à la lettre tout ce qu'on a dit jusqu'ici, même si les idées émises vous semblent pertinentes et leur mise en application nécessaire. Entre une nécessaire sécurité de l'Information et une menace d'inculpation d'espionnage ou d'atteinte à la sécurité de l'état, entre ne pas chiffrer et la prison ou l'expulsion, il faut choisir…

Un autre cas où il ne convient pas de chiffrer est celui où les performances, suite au chiffrement, ne sont pas celles que l'on est en droit d'espérer. Certains éditeurs de bases de données, par exemple, déconseillent de chiffrer les enregistrements à mettre dans leur base. Ce n'est pas que la fonction chiffrement est lente, avec les ordinateurs d'aujourd'hui, mais s'il faut, suite à une requête, déchiffrer un nombre incroyable d'enregistrements inutiles pour parvenir au résultat que l'on cherche, il est sûr qu'il vaut mieux éviter de chiffrer, qu'on soit d'ailleurs dans un cloud on qu'on reste chez soi.

EN CONCLUSION

Nous l'avons souligné, la question est très bonne et on ne peut y répondre par oui ou par non. Ce qui se dégage est que le chiffrement des informations confidentielles ou nominatives, dans un cloud mutualisé, semi public ou public est indispensable s'il est possible. Mais il ne dispense pas l'utilisateur de la responsabilité de protéger ses informations. La gestion des clés de chiffrement se pose. Nous avons vu également que le canal entre le prestataire du cloud et l'utilisateur doit être chiffré, et que moins vous gardez la gouvernance sur vos données, plus vous avez intérêt à les signer.

Et pour finir la conclusion :

Avant de sauter dans le nuage, mieux vaut prévoir un parachute !

A PROPOS DE L'AUTEUR

Gérard Peliks est expert sécurité dans le Cassidian Cyber Security Cassidian est la division « Defense and Security » d'EADS.

Il préside l'atelier sécurité de l'association Forum ATENA, et coordonne l'activité sécurité de l'Information du Cercle d'Intelligence Économique du Medef Ile-de-France.

Il est chargé de cours sur différentes facettes de la sécurité, dans le cadre de mastères à Telecom ParisTech et dans d'autres écoles d'Ingénieurs. A l'ISEP, il intervient sur des modules sécurité dans le cadre des mastères spécialisés et a participé au comité de pilotage du mastère professionnel Intelligence des Risques.