Executive Certificate Cloud Computing

Le cloud computing et l'enjeu de la sécurité

Octobre 2018

Ahmed Mekaouar

Remerciements

Je tiens à remercier Pierre-Fréderic Rouberties, le responsable de la formation Executive Certificate Cloud Computing, ainsi que tous les intervenants des différents modules pour la qualité et la richesse du contenu proposé. Ils ont tous contribué à ce travail en me transmettant à la fois leur passion et leurs vastes connaissances du cloud computing et de ses enjeux!

Table des matières

1 Introduction

Le cloud a révolutionné le rapport de l'entreprise à son système d'information en lui permettant l'accès à de l'infrastructure et à des applications avec peu ou pas d'investissement. Depuis l'apparition des premières offres entreprise comme Amazon S3 en 2006, le cloud n'a cessé de gagner du terrain. Phénomène de mode à ses débuts, le cloud a maintenant dépassé ce stade pour devenir une priorité stratégique, aussi bien pour les grands groupes que pour les PME. Selon une étude[1] réalisée en 2016, 21% des entreprises en Europe ont fait appel à des services cloud et la moitié d'entre elles a fait appel au cloud pour des applications avancées tels que la gestion de relation client. Il ressort également de cette étude que beaucoup d'entreprises hésitent à franchir le cap et celles qui utilisent le cloud limitent leurs usages à certains types d'applications. Les entreprises, qui n'utilisent pas le cloud, évoquent une méconnaissance des technologies et du modèle cloud ainsi que du cadre contractuel et légal qui peut régir la relation avec les fournisseurs. Celles qui limitent leur utilisation ont des inquiétudes concernant la sécurité dans le cloud, des questions par rapports aux lois applicables et des doutes par rapport à la localisation des données.

Si le cloud n'a cessé de prendre du terrain, les attaques de sécurité qui le ciblent augmentent à un rythme beaucoup plus important. Ces dernières ont augmenté de 300% entre 2016 et 2017[2]. Cette cybercriminalité est un réel frein pour les entreprises qui souhaitent profiter du cloud comme accélérateur d'innovation et moyen de réduire les coûts. Son augmentation est en partie due à une méconnaissance du modèle cloud, de ses spécificités et leurs répercussions sur la sécurité de l'information.

Ce mémoire se place du côté du client ou de l'utilisateur qui souhaite connaitre les spécificités du cloud d'un point de vue sécurité et obligations légales. Ce travail tente avant tout d'engager la réflexion du client, lui faire prendre conscience de ses responsabilités et lui proposer une approche afin de mesurer et gérer les risques relatifs à une transition vers le cloud. Le mémoire propose également un ensemble de bonnes pratiques et de mesures qui peuvent être mises en place afin d'améliorer la sécurité du système d'information et se conformer aux règlementations en vigueur.

[1] http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises
[2] https://www.secureworldexpo.com/industry-news/attacks-on-cloud-2017

1.1 Le cloud computing

Selon le NIST, le cloud computing est un modèle qui permet un accès à la demande à des ressources partagées (réseaux, serveurs, stockages, services, applications) à travers le réseau. Ces ressources sont provisionnées rapidement et libérées sans effort et avec un minimum d'interaction avec le fournisseur. Il a les 5 caractéristiques suivantes :

- Il doit être en libre-service à la demande.
- Il doit être accessible par internet.
- Il doit y avoir une mutualisation des ressources.
- Il doit être rapidement élastique.
- Il doit être mesurable.

Nous allons par la suite voir les différents modèles de service, modèles de déploiement et acteurs du cloud et nous allons essayer de comprendre le partage de responsabilités relatif au modèle du cloud computing.

1.1.1 Modèles de service

Toujours selon le NIST, il y a 3 niveaux de service :

- Le SaaS (*Software as a Service*) : Il s'agit d'un logiciel sous la forme d'une application généralement accessible à partir d'un navigateur web et qui offre un service particulier comme la messagerie par exemple. Dans ce modèle le client ne gère que la configuration de l'application. Gmail de Google est l'un des premiers SaaS largement adopté par le grand public.

- Le PaaS (*Platform as a Service*) : Il s'agit d'une solution qui propose environnement de développement avec un ensemble d'outils de libraires et de services. Cloud Foundry est un exemple de PaaS et il s'agit d'une plateforme d'intégration continue. Ce modèle offre un peu plus de flexibilité que le SaaS vu qu'il est possible au client de développer ses propres applications mais le client reste tout de même limité par l'environnement proposé.

- L'IaaS (*Infrastructure as a Service*) : Dans ce modèle le client provisionne des ressources matérielles comme la capacité de stockage et capacité de calcul à la demande sur un réseau. Le service de stockage Amazon S3 lancé en 2006 peut être considéré comme la première offre IaaS en cloud public. L'IaaS est le modèle qui offre le plus de contrôle au client qui peut utiliser l'infrastructure provisionné selon son besoin et sans restriction. Ce niveau de contrôle élevé implique également que le client est responsable de gérer la maintenance et l'évolution de son système d'information.

1.1.2 Modèles de déploiement

Le choix d'un service cloud s'accompagne également du choix du mode du déploiement.

- Le cloud public : Les offres de cloud public sont ouverts à un large public à savoir les particuliers, les entreprises, les différentes organisations publiques ou privées. Un cloud public donnée est la propriété d'un fournisseur de services cloud. C'est le fournisseur qui opère et contrôle l'infrastructure et les services proposés. Les ressources proposées par le cloud public sont alors en dehors du périmètre du client et sont partagés entre tous les clients potentiels.

- Le cloud privé : Le cloud privé offre les mêmes services qu'en cloud public mais il est la propriété d'une organisation donnée. Les ressources ne sont pas ouvertes à un public large mais partagées uniquement entre différentes entités de cette organisation. Le cloud privé peut être opéré par l'organisation elle-même ou par un sous-traitant. Le cloud privé offre un niveau de control plus grand que le cloud public mais l'organisation doit assumer les dépenses nécessaires pour acquérir et opérer l'infrastructure.

- Le cloud communautaire : Ce cloud est accessible par un groupe d'organisations qui partagent des objectifs et des contraintes similaires. Les ressources sont alors mutualisées entre organisations. C'est un modèle de déploiement entre le cloud public et le cloud privé.

- Le cloud hybride : Le cloud hybride est la combinaison de deux modèles de déploiements parmi ceux vus précédemment. Il est possible par exemple d'utiliser de stocker certaines données critiques dans le cloud privée et de faire appel à un cloud public pour d'autres applications.

1.1.3 Acteurs du cloud

L'architecture de référence adoptée par le NIST définit 5 types d'acteur dans un environnement cloud. Ils ont des rôles et des responsabilités différentes.

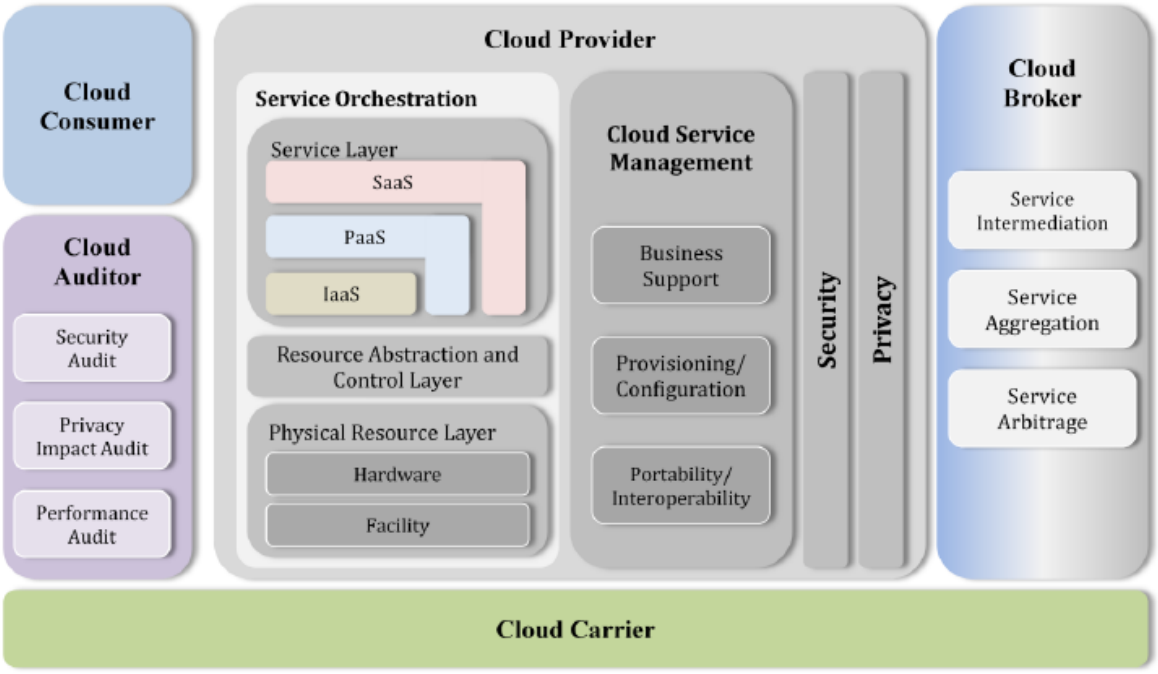

Figure 1- Architecture de référence : Les acteurs du cloud (NIST SP 500-292)

- Le client cloud (*cloud consumer*) : C'est une personne ou une organisation qui fait appel à un service fourni par un fournisseur cloud.
- Le fournisseur cloud (*cloud provider*) : C'est une personne ou organisation qui met un service cloud à disposition des clients potentiels.
- L'auditeur cloud (*cloud auditor*) : C'est un tiers qui évalue le service cloud en termes de performances et de mesures de sécurités en place.
- L'intermédiaire cloud (*cloud broker*) : C'est une entité qui gère l'utilisation, la performance des services cloud. C'est lui qui sert d'intermédiaire entre le client et le fournisseur et peut offrir certains services tels que la gestion d'identité ou l'amélioration de la sécurité. Il peut également négocier et sélectionner les bonnes offres afin de répondre au besoin du client. Il n'est pas obligatoire de passer par intermédiaire mais cela peut être utile pour les organisations qui ne souhaitent pas traiter avec le fournisseur cloud directement.
- Le fournisseur d'accès (*cloud carrier*) : C'est l'entité qui fournit l'accès à internet afin de donner accès au service cloud. Le SLA d'un fournisseur de cloud dépond directement du SLA de son fournisseur d'accès.

1.1.4 Responsabilité de la sécurité dans le cloud

Les offres cloud sont certes de plus en plus utilisées mais il subsiste toujours une méconnaissance chez certains dirigeants quant aux responsabilités de chacun pour assurer la sécurité du système. Les résultats d'une enquête[3] indiquent que 76% des organisations considèrent que « le fournisseur d'accès cloud s'occupe entièrement de protéger la confidentialité des données et d'assurer la conformité aux réglementations en vigueur ». Ceci est bien évidemment faux et quel que soit le modèle de service adopté. Nous sommes plutôt sur un schéma de responsabilité partagée avec un degré de responsabilité proportionnel au degré de contrôle.

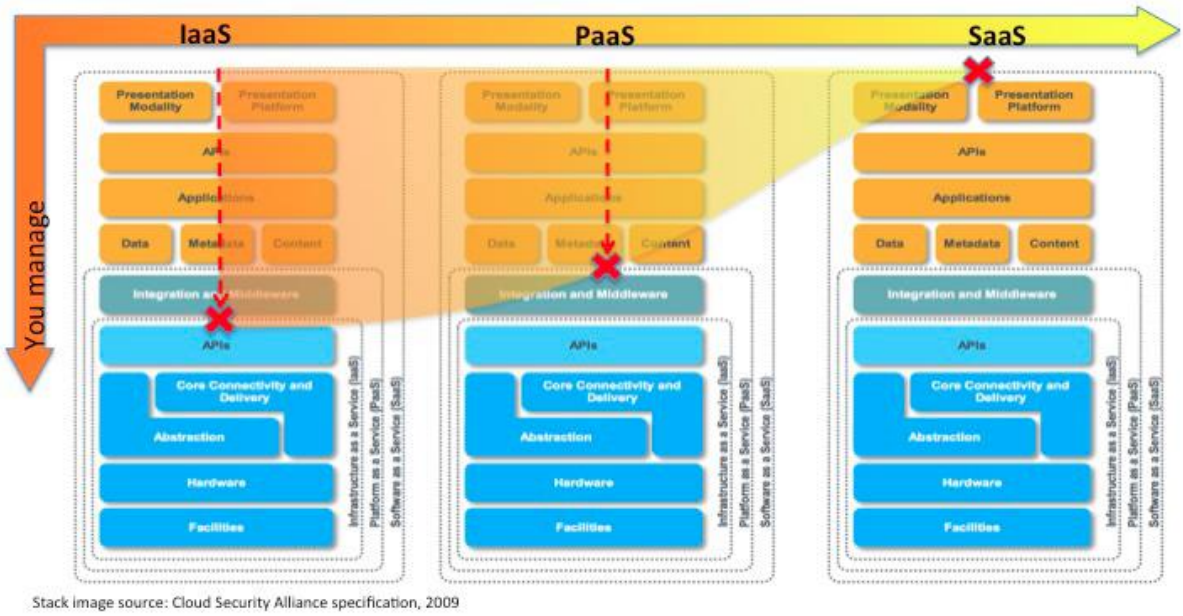

Figure 2 – Responsabilités et modèles de service[4]

Sous le modèle SaaS, le client est simple consommateur de l'application. C'est le fournisseur cloud qui contrôle toutes les couches. Le contrôle du client se résume à de la configuration selon ce que propose le fournisseur. Malgré ce niveau de contrôle faible, le client n'est pas dispensé de certaines mesures et pratiques nécessaires à la sécurité des données. Parmi les ces mesures, on peut lister la gestion d'identité et des accès, la gestion de la sécurité des données et la gestion de la conformité aux réglementations. C'est au client de décider s'il doit ou pas activer le chiffrement des données au repos par exemple. Il peut également mettre en

[3]https://www.veritas.com/form/whitepaper/the-truth-in-cloud

[4]https://www.nist.gov/publications/cloud-computing-security-foundations-and-challenges-chapter-14-cloud-computing-security

place un système de prévention de perte de données (*Data Loss Prevention*) s'il juge que c'est nécessaire. En d'autres termes, le client même en mode SaaS, ne doit pas se contenter de la protection par défaut mais il doit activer les bonnes configurations et mettre en place les bonnes mesures afin de répondre à son besoin en termes de sécurité. Les fournisseurs de services SaaS ne connaissent à priori pas la criticité des données et il n'est pas de leur ressort de décider des mesures de protections requises pour les stocker. Même si certains d'entre eux proposent des outils pour sécuriser les données, il est de la responsabilité du client d'activer une telle fonctionnalité et de vérifier si elle répond au besoin déjà établi lors de la phase de classification des données. A titre d'exemple, Salesforce[5] propose une solution de chiffrement pour les données au repos mais c'est au client de s'assurer que cette solution correspond à ses besoins et de l'activer le cas échéant. Cette protection (le shield de Salesforce) peut s'avérer insuffisante s'il y un besoin de confidentialité quand les données sont en utilisation par exemple.

Sous les modèles PaaS/IaaS, le client est responsable également des applications. AWS, qui est essentiellement un fournisseur IaaS, propose le partage suivant des responsabilités :

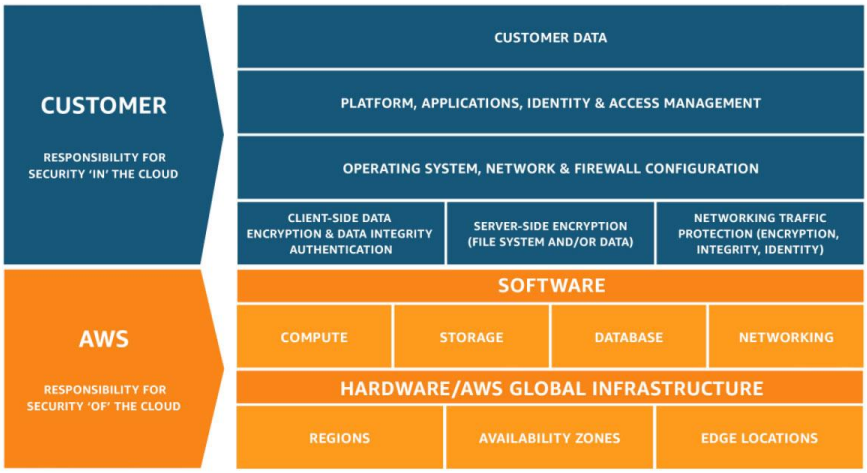

Figure 3- Partage des responsabilités AWS

AWS se définit comme responsable de la sécurité du cloud (*of the cloud*) et désigne le client comme responsable de la sécurité dans le cloud (*in the cloud*). En d'autres termes, AWS est responsable du cloud en tant qu'infrastructure et le client est responsable de la sécurité des données, de la gestion d'identité, de la sécurité des applications, de la configuration du Firewall et du réseau, du système d'exploitation etc…

[5]https://www.salesforce.com/products/platform/products/shield/

1.2 Sécurité du système d'information

La sécurité est un enjeu majeur pour tout système d'information, y compris dans le cloud. Voici un aperçu sur l'objectif de la sécurité du SI, le profil des cybercriminels, les types de menaces ainsi que les catégories de mesures de contrôle.

1.2.1 La sécurité du SI

La sécurité du système d'information vise à garantir la **Confidentialité**, l'**Intégrité** et la **Disponibilité** de l'information. Ces trois principes forment la triade CIA (*Confidentiality*, *Integrity*, *Availability*) qui est la base de la sécurité.

- La confidentialité fait en sorte que seules les personnes ou entités autorisées peuvent avoir accès aux données. La cryptographie et le contrôle d'accès sont les méthodes principales afin de garantir la confidentialité.
- L'intégrité vise à garantir que les données n'ont pas été modifiées ou corrompus. La cryptographie peut nous aider pour atteindre cet objectif.
- La disponibilité concerne les données et les applications. Ces derniers doivent être accessibles pour tout utilisateur légitime. Afin de garantir cet objectif, il faut mettre en place des systèmes de redondance et de backup pour les données et de répartition de charge (*load balancing*) pour les applications.

1.2.2 Les cybercriminels

Les menaces et attaques qui visent le cloud proviennent de sources différentes et ont des motivations variées. Voici un aperçu sur les cybercriminels et leurs motivations :

- Le *Script Kiddie* est un attaquant ayant peu de compétence en réseau et en sécurité informatique. Il utilise des scripts faits par d'autres afin de lancer ses attaques. Malgré le manque de compétence, il peut être un danger réel s'il met la main sur des outils puissants. Il peut être motivé par l'argent mais aussi par la gloire d'y arriver!
- Le *Hacktiviste* ou le cyberactiviste lance son attaque afin de défendre ou attirer l'attention sur une cause idéologique ou politique.
- L'*Insider* : C'est l'auteur d'une menace de l'intérieur d'une organisation. L'acteur en question dispose généralement de certains privilèges et droits d'accès. Il peut être malicieux ou non. L'acteur malicieux peut être motivé par l'argent ou par la vengeance contre la structure. Dans le cas du cloud, nous avons affaire à deux types d'Insider : celui de l'entreprise et celui du fournisseur de services cloud.

- Les compétiteurs : Ils peuvent lancer des attaques avec comme principal but d'obtenir des informations confidentielles et propriétaires.
- Le crime organisé : Il est une des plus dangereuses sources de menaces avec le gain financier comme principale motivation.
- Les gouvernements : Ils peuvent être les sponsors de menaces persistantes avancées (APT : *Advanced Persistent Threat*). Ces attaques sont généralement sophistiquées et ciblés vu les énormes moyens dont disposent les attaquants.

1.2.3 Les menaces

Il est possible de classer les menaces selon le modèle STRIDE proposé par Microsoft[6].

Ce modèle distingue 6 types de menaces qui sont les suivants :

- ***S**poofing* (Userpation d'identité) : C'est le fait qu'un utilisateur malicieux se fasse passer pour un utilisateur légitime et obtenir ainsi un accès à des ressources auxquelles il n'a normalement pas accès.
- ***T**ampering* (Falsification) : Cela consiste à modifier ou supprimer une ressource sans autorisation.
- ***R**epudiation* (Répudiation) : La répudiation est le fait de nier avoir reçu ou envoyé certaines informations ou avoir été à l'origine d'une transaction ou de toute autre communication sur le réseau.
- ***I**nformation Disclosure* (Divulgation de l'information) : Il s'agit d'une menace visant la confidentialité des données.
- ***D**enial of Service* (Déni de Service) : une attaque par Déni de Service a pour but de rendre indisponible les données ou les applications qui forment le système d'information.
- ***E**levation of Privilege* (Elévation de privilège) : L'élévation de privilège est le fait obtenir un niveau d'autorisation plus élevé que celui prévu initialement.

1.2.4 Les mesures de sécurité

Afin de réduire le risque des menaces ci-dessus, il existe plusieurs mesures de sécurité. Ces mesures peuvent être classées en 3 types : Les mesures techniques, les mesures administratives et les mesures physiques.

[6]https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v%3dcs.20)

➢ *Mesures techniques*

Les mesures techniques sont implémentées à l'aide de la technologie. Il est possible de lister à titre d'exemple : Le chiffrement, l'anti-virus, le firewall et les systèmes de détection d'intrusion.

➢ *Mesures administratives*

Les mesures administratives peuvent découler d'une politique de sécurité d'entreprise. Ces mesures incluent entre autres :

- Audit des vulnérabilités : Cet audit permet de découvrir les vulnérabilités du système. Cette étape permet de préparer l'analyse des risques.
- Analyse et gestion des risques : L'analyse des risques permet d'estimer et classer les risques afin de les gérer en fonction de la criticité.
- Formation des employés : L'utilisateur final est considéré comme le maillon faible de la sécurité. Il est essentiel de bien former les employés afin qu'ils prennent conscience des menaces et qu'ils adoptent les bonnes pratiques de sécurité.

➢ *Mesures physiques*

La sécurité physique rassemble toutes les mesures afin de protéger physiquement les données. Ces mesures sont de la responsabilité du fournisseur de services cloud.

2 Cycle de vie des données

Nous adopterons tout au long de ce travail une approche centrée sur les données. Nous proposons un cycle de vie en six états plus un état de transit:

Figure 4- Cycle de vie de la donnée

2.1 Création des données

Cette première étape consiste à la construction de nouvelles données ou l'acquisition de données existantes. Il est important, dès la création des données, de les classifier selon la politique interne de l'organisation et les réglementations en vigueur. Cette classification a comme objectif de nous permettre de déterminer des mesures de sécurités à mettre en place afin de protéger ces données. Une mauvaise classification des données peut menacer leur sécurité et exploser ainsi l'entreprise à des risques financiers, des problèmes de conformité et de perte de confiance des clients ou des partenaires.

2.2 Stockage des données

Une fois les données créées, il faut choisir une solution de stockage. La classification déjà effectuée au moment de la création nous aide à choisir le mode de stockage et le niveau de sécurité requis pour les données. Par exemple, les données de santé en France ne peuvent être stockées que chez un fournisseur agrée[7].

Selon le type des données, il peut être nécessaire de mettre en place les mécanismes afin de protéger la confidentialité et l'intégrité des données et s'assurer qu'elles soient disponibles selon le besoin.

2.3 Utilisation des données

Une fois stockées, les données peuvent être accédées et traitées. S'il s'agit de données chiffrées au repos, elles vont probablement être déchiffrées afin de permettre le traitement. C'est une phase où les données sont vulnérables. Si les données en utilisation sont accessibles par une application, il faut veiller à ce que cette application suive un cycle de vie sécurisé. Il faut également restreindre l'accès aux seuls utilisateurs autorisés et ayant réellement besoin de cet accès pour remplir leur mission.

2.4 Partage des données

Les données peuvent être partagées avec des partenaires ou des sous-traitants. Il s'agit également d'un point de vulnérabilité. Ce partage présente un nouveau vecteur de menace pour les données de l'organisation. Encore une fois, la classification des données peut aider à déterminer celles qui sont susceptibles d'être partagées et avec quelles parties. Il faut également

[7]http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees

exiger de ses partenaire et sous-traitants de mettre en place des mécanismes pour minimiser les risques de fuites de données telles que les systèmes de prévention de fuite de données DLP (*Data Loss Prevention*).

2.5 Archivage des données

Certaines données peuvent perdre de la valeur selon le cas d'utilisation et il peut être pertinent de les archiver afin de garantir une gestion optimale des ressources. Il s'agit d'une phase plus au moins longue avant la destruction définitive. Selon les données, il peut être nécessaire d'appliquer les mêmes mesures de sécurité que pour le stockage classique. Des données à caractère personnel ou de santé par exemple doivent être chiffrés même quand elles sont archivées.

2.6 Effacement des données

Quand les données n'ont plus de raison d'exister dans le système ou suite à une obligation légale, elles sont supprimées. Il est important que l'effacement se fasse de manière sécurisée afin de s'assurer que les données sont irrécupérables. Il est difficile dans le cas du cloud, de s'assurer de l'effacement des données. C'est le fournisseur de cloud qui opère l'infrastructure et il n'y a généralement pas de garantie de l'effacement réel des données dans ce contexte. Ceci dit, des solutions existent et peuvent nous aider à adresser ce problème.

2.7 Transit des données

Les données se déplacent dans le réseau tout au long de leur cycle de vie. Ceci est d'autant plus vrai dans une architecture cloud qui fait intervenir plusieurs parties. Il est donc indispensable de veiller à ce que les données transitent de manière sécurisée dans le réseau.

3 Gouvernance des données

Si les organisations sont conscientes de l'importance des données, et les mettent au cœur de leur stratégie, la plupart[8] ne sont pas capables de de localiser les données critiques au sein de leur système d'information et ils ne savent pas ce qu'il faut faire pour les protéger. Cette absence de gouvernance pose à la fois des problèmes en termes de stratégie, de sécurité des données et de conformité aux réglementations comme le RGPD.

[8]Thycotic, The 2017 State of cybersecurity metrics annual report

3.1 Classification des données

Les données sont de plus en plus collectées par les entreprises. Ces dernières ont tendance à vouloir récupérer et garder le plus de données que possible dans l'espoir de créer de la valeur grâce aux technologies Big data. Afin d'atteindre cet objectif, il est indispensable de classifier les données au plutôt et idéalement dès la création ou l'acquisition. Cette classification permet alors d'identifier les données stratégiques, les données sensibles ou autres types afin de mettre en place les bons mécanismes de sécurité. Le principe consiste alors à identifier des groupes de données qui partagent des caractéristiques semblables ou des risques communs et d'identifier le niveau de sécurité nécessaire à chaque groupe. Voici un résumé des étapes[9] qui permettent de mettre en place une classification efficace des données :

- Analyse des risques : Cette étape consiste à comprendre les obligations légales ou contractuelles de l'organisation auxquelles l'organisation est soumise. Ceci permet de définir les objectifs de la classification surtout d'un point de vue sécurité des données.
- Politique de classification : Elle consiste à définir les niveaux de classification des données selon le degré de confidentialité et les contraintes en termes de sécurité. Le tableau suivant propose une politique de classification type qui peut servir de base, en ayant à l'esprit qu'il faut garder un nombre raisonnable de niveaux pour ne pas trop complexifier le système. Il faut également prévoir les mesures de sécurité à mettre en place en s'appuyant notamment sur l'analyse des risques réalisée au préalable.

Public	**Interne**	**Confidentiel**	**Restreint**
Données qui peuvent être partagées en public. Par exemple : - Tarifs - Contact entreprise - Communication du marketing	**Données à usage interne et non destinées au public.** Par exemple : - Organisation - Chiffres des ventes - Stratégie concurrentielle	**Données dont la violation peut nuire aux intérêts de l'organisation.** Par exemple : - Contrats avec les fournisseurs - Dossiers des performances des employés	**Données dont la violation représente un grand risque financier ou/et légal**. Par exemple : - Données à caractère personnel - Données de santé - Données financières

Tableau 1- Exemple de politique de classification

[9]https://focus.forsythe.com/articles/619/7-Steps-to-Effective-Data-Classification

- Bilan des données collectées et traitées : L'organisation doit avoir une bonne visibilité des données collectée et des clients et partenaires concernés par cette collecte.
- Localisation des données : Il faut que l'organisation puisse avoir une bonne visibilité de la localisation de ses données. Il faut prêter une attention particulaire aux services cloud qui peuvent être utilisées parfois d'une manière officieuse (*Shadow-IT*). L'utilisation des appareils mobiles au sein de l'entreprise doit être également prise en compte.
- Classification des données : Une fois les données identifiées et localisées, elles doivent être classées selon la politique mise en place précédemment.
- Mesures de sécurité : Elles doivent être mises en place selon les classes définies.
- Maintenance et contrôle : Tout ce processus doit être maintenu et revu afin de s'adapter à de nouveaux besoins ou à des changements dans l'environnement de l'organisation.

3.2 Sécurité des données

La classification des données, détaillée précédemment, permet d'alimenter la politique de sécurité afin de refléter toutes les mesures de sécurité spécifiques pour chaque classe de données. La politique de sécurité peut par exemple exiger que seules des données classées sous le niveau 'public' peuvent être stockées chez un fournisseur de services cloud.

Certaines données sont critiques à la mission de l'organisation. Ceci doit être pris en compte dans le plan de reprise d'activité (*Business Recovery Plan*). Il conviendrait alors de mettre en place un système de réplication ou de backup afin de permettre une reprise d'activité en cas d'incident.

3.3 Politique de collecte et de rétention des données

A l'ère du Big Data, les entreprises collectent de plus en plus de données et peuvent facilement être confrontées à un manque de contrôle et de visibilité. Il est dans l'intérêt de l'entreprise d'avoir une réflexion sur les cas d'utilisation et de ne collecter que les informations nécessaires aux traitements souhaités afin d'éviter de se retrouver avec des données stockées mais non utilisées.

Une organisation n'a ni intérêt, et parfois, ni le droit de stocker les données sans finalité et politique de rétention claire. D'une part, certaines informations perdent naturellement leur valeur stratégique au bout d'un certain temps. D'autre part, et pour une question de droit, l'entreprise peut être amenée à effacer certaines données au bout d'un certain temps ou, au contraire, à garder certaines données pour une durée minimale. Il est alors nécessaire que la

politique de rétention des données soit mise en place et implémentée afin de garantir à la fois une utilisation optimale des ressources et le respect des réglementations en vigueur.

3.4 Responsabilités

La gouvernance des données nécessite une certaine cohérence et il n'est pas possible de l'assurer que de manière centralisée. Un des rôles clés est celui du directeur des données ou CDO (*Chief Data Officier*). Il est responsable de la mise en place la politique de classification des données et des mesures de sécurité nécessaires pour la protection des données. Dans le cadre du RGPD, il joue alors le rôle de délégué à la protection des données ou DPO (lorsque ce rôle est obligatoire) et doit ainsi veiller à ce que la règlementation soit respectée et appliquée au sein de son organisation.

4 La politique cloud

Avoir une politique cloud claire peut être considéré comme la première étape afin de construire la sécurité d'un système d'information cloud. Certaines directions d'entreprises omettent de faire la réflexion à propos du cloud et laissent alors la porte ouverte à une utilisation à risque. Les métiers peuvent alors décider d'utiliser un service cloud qui répond à leur besoins en mettant en place une infrastructure de type *Shadow IT*. Adopter un service cloud dans un tel cadre présente généralement un risque pour la sécurité de l'organisation.

4.1 Le cloud et la stratégie d'entreprise

Avant de se lancer dans le cloud, il faut s'assurer qu'un tel choix s'inscrive dans une stratégie globale et une vision cohérente. Les services cloud ne proposent pas de réponses génériques mais répondent à des besoins spécifiques. Il faut alors que l'entreprise se pose d'abord la question de savoir pourquoi elle veut aller dans le cloud afin de valider le besoin d'une telle transition. A l'issue d'une telle réflexion, une entreprise peut formuler une stratégie d'adoption du cloud selon ses contraintes et ses intérêts. Si certaines entreprises ont tout intérêt à adopter une stratégie 'tout cloud', d'autres peuvent choisir une stratégie 'IT traditionnel' ou hybride. Ces choix ont bien entendu des répercussions en termes de sécurité du système d'information. Il est alors indispensable de bien évaluer les menaces et les risques auquel l'organisation s'expose si elle décide d'avoir recours à tel ou tel service cloud.

4.2 Analyse et gestion des risques dans le cloud

L'analyse des risques est une étape importante de la gestion des risques. Elle permet de quantifier ou qualifier les risques en se basant sur différents critères. Pour ce faire, il est indispensable de se poser la question des **biens** à protéger. Il faut alors lister l'ensemble des données, des applications et des processus qu'on souhaite protéger. Il faut également essayer de donner une valeur quantitative ou qualitative à ces biens. Cette valeur nous aidera par la suite à évaluer l'impact d'un tel ou tel scenario. L'analyse des risques identifie alors les **menaces** et les **vulnérabilités** et détermine la probabilité qu'une menace puisse exploiter une vulnérabilité.

Dans ses recommandations[10] pour l'analyse des risques du cloud computing, l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) propose une liste de biens, de menaces et de vulnérabilités. Elle suggère d'estimer le niveau du risque en se basant sur la probabilité d'un scenario et de son impact business.

Les scenarios de risques définis par l'ENISA sont groupés en trois catégories : Politique & organisationnel, Technique et Légal. La probabilité de chaque scenario et l'impact business sont déterminés par un groupe d'experts. Le modèle proposé est qualitatif. Les grandeurs ***Probabilité du scenario*** et ***Impact business*** sont des valeurs discrètes sur une échelle allant de 1 à 5 (de 'très bas' à 'très élevé'). Le risque est calculé comme étant la somme des deux grandeurs. Le risque est une valeur qualitative codée comme suivant :

0-2 : Risque faible

3-5 : Risque moyen

6-8 : Risque élevé

	Probabilité du scenario	Très basse	Basse	Moyenne	Elevée	Très élevée
Impact Business	Très bas	0	1	2	3	4
	Bas	1	2	3	4	5
	Moyen	2	3	4	5	6
	Elevé	3	4	5	6	7
	Très élevé	4	5	6	7	8

Tableau 2- Estimation du risque (ENISA)

[10]Cloud Computing BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY - ENISA

L'ENISA fournit une liste de 53 vulnérabilités, dont 31 sont spécifiques au cloud, et de 23 type de biens que fournisseur ou client peuvent mettre dans le cloud. L'ENISA liste également 35 scenarios d'incidents. Chaque scenario est associé à un sous ensemble de vulnérabilités et de biens. Voici à titre d'exemple les vulnérabilités et les biens associés au risque R1 Lock-in fournisseur :

Probabilité	Elevée	Comparé à l'IT traditionnel : Plus élevée
Impact	Moyen	Comparé à l'IT traditionnel : Même chose
Vulnérabilités	V13. Absence de technologies standards V46. Mauvais choix de fournisseur V47. Absence de fournisseurs multiples V31. Manque de transparence de la part du fournisseur	
Biens affectée	A1. Réputation de l'entreprise A5. Données personnelles sensibles A6. Données personnelles A7. Données personnelles critiques A9. Livraison de services temps réel A10. Livraison de services	
Risque	**Moyen**	

Tableau 3- Scenario du risque : lock-in fournisseur

Les risques étant nombreux, cette approche peut s'avérer très utile afin de classer les différents scenarios et de se concentrer ainsi sur la gestion des risques les plus importants. Il faut alors déterminer les mesures à mettre en place afin de minimiser chaque risque.

Ceci dit, si les experts sont capables d'estimer l'impact du scenario d'un risque, il leur est parfois difficile de donner une estimation de la probabilité de certains risques dont on ne maitrise pas les facteurs déclenchants. Ces estimations sont alors plutôt guidées par l'expérience et les évènements passés et ne tiennent parfois pas compte de la réalité de la situation. Il est également impossible d'identifier les risques liés aux vulnérabilités inconnues (*Zero Day*) au moment de l'analyse. Il faut alors être conscient que cette démarche d'analyse et de gestion des risques ne met pas forcement à l'abri de tous les dangers.

Afin d'en tirer le maximum, cette démarche doit également s'inscrire dans la durée. Il est essentiel de refaire l'exercice régulièrement afin de tenir compte de nouvelles vulnérabilités et des nouvelles données ou applications qu'on souhaite héberger dans le cloud.

4.3 Transition vers le cloud

Le cloud concerne aussi bien les entreprises qui démarrent en 'tout cloud' que les celles qui fonctionnent avec un système d'information traditionnel. Ces dernières peuvent avoir intérêt à migrer une partie de leur activité vers le cloud afin de gagner en agilité ou de rationaliser les dépenses en infrastructure. Ces entreprises doivent alors bien se préparer pour bien gérer leur transition vers le cloud. Cette préparation implique toutes les étapes vues précédemment. Il faut alors engager une réflexion sur la cohérence du cloud avec la stratégie globale et analyser les risques relatifs au modèle du cloud computing. Les entreprises peuvent privilégier les systèmes les moins critiques en termes de sécurité pour commencer leur transition vers ce modèle. Il est courant de voir les fonctions de support migrer en premier via des applications SaaS. Cela permet de familiariser l'entreprise avec ce nouveau modèle pour faire par la suite des projets plus ambitieux. Si certaines structures peuvent viser le 'tout cloud', cette cible n'est surement pas raisonnable pour toutes. Il est essentiel de peser les avantages et les inconvénients et de faire les bons choix en fonction des contraintes et des objectifs de la structure.

4.4 Choix des fournisseurs

Il faut se poser la question du choix du service et du fournisseur pour chaque besoin. Il n'y a pas solution standard qui puisse satisfaire tous les cas d'utilisation. Le client doit partir de ses besoins, de ses exigences et des contraintes légales afin de choisir la solution qui lui convient. L'article 28 du RGPD inscrit la responsabilité du client dans le choix du fournisseur cloud. Le client « fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles… »

L'évaluation du fournisseur cloud passe par une analyse fine du service et des différents SLAs afin de vérifier si l'offre correspond bien au besoin. Il faut également se poser certaines questions comme celle de la gestion de la fin du contrat et de la réversibilité des données. Il est indispensable d'identifier et évaluer les risques associés à chaque fournisseur afin d'éclairer le choix.

4.5 Le cloud et la politique de sécurité

Etablir une politique cloud claire permet de poser une première brique pour bâtir la sécurité d'un système d'information dans le cloud. Une politique cloud implique souvent un changement dans la politique de sécurité afin de gérer les risques liés aux nouveaux usages. Cette politique de sécurité rassemble toutes les mesures techniques ou administratives qu'il est convenable de mettre en place pour protéger les données externalisées vers le cloud. A titre d'exemple, cette politique peut exiger le chiffrement systématique des données à caractère personnel dans le cloud tout en gardant la main sur la gestion de l'infrastructure des clés publiques.

Plusieurs mécanismes peuvent aider à faire appliquer une politique de sécurité adaptée à l'usage du cloud :

- Communication et sessions de formations : Il est essentiel que la politique de sécurité cloud soit bien communiquée et expliquée à l'ensemble du personnel concerné. Il est indispensable de sensibiliser les utilisateurs aux risques liés à l'usage du cloud et leurs suggérer les bonnes pratiques à adopter.
- Les enregistrements (*logs*) peuvent servir à établir les actions des utilisateurs. Un système d'enregistrement bien sécurisé (qui garantit l'intégrité) peut être un moyen pour garantir la non-repudiation d'une action de la part d'un utilisateur.
- L'utilisation de *Cloud Access Security Brocker* (CASB): Il s'agit d'un outil logiciel installé en local ou d'un service cloud qui permet d'appliquer une politique de sécurité cloud. Il est placé entre le client cloud et les fournisseurs de services cloud. Il peut alors contrôler le trafic réseau et faire appliquer mesures de sécurités liées au cloud.

5 Facteurs de risques relatifs au cloud

5.1 Disparition du périmètre IT

La sécurité du système d'information classique s'est construite autour et à l'aide du périmètre maitrisé qui est celui de l'organisation. Ce périmètre protégé permettait alors de protéger les données qui sont à l'intérieur de la structure. Ceci dit, cette défense périmétrique n'a jamais été efficace contre les menaces internes (*Insider*) et elle a de plus en plus de mal à protéger les données dans un environnement connecté et des utilisateurs et des équipements mobiles. L'adoption du cloud et le stockage des données hors périmètre classique rendent la sécurité traditionnelle obsolète et pose un énorme défi aux dirigeants et aux responsables de

sécurité. Avec la disparition du périmètre et le recours à la virtualisation, les applications et les données d'un client peuvent se retrouver sous la même machine physique que celles d'un autre client.

5.2 Virtualisation des serveurs

L'utilisation efficiente des ressources est une des propriétés fondamentales du modèle cloud. La virtualisation des serveurs s'est alors naturellement imposée vu qu'elle permet une utilisation optimale des machines physiques. Deux machines virtuelles lancées par deux clients différents peuvent alors tourner sur un même serveur physique. Cette isolation logique des utilisateurs n'est malheureusement pas sans risque. Un utilisateur malicieux d'une machine virtuelle peut lancer une attaque d'évasion de VM (*VM escape*). S'il réussit, il peut contrôler le système hôte et avoir un niveau de privilège élevé, ce qui expose toutes les machines virtuelles qui tournent sur la machine physique.

Les fournisseurs de services cloud sont les principaux responsables de la sécurité de l'infrastructure en général et des machines virtuelles en particulier (lorsque la VM fait partie du service). Les gros fournisseurs, tels qu'AWS, Azure ou Google Cloud Platform, sont assez sérieux par rapport à la sécurité et appliquent les correctifs assez régulièrement. Ceci dit, le risque zéro n'existe pas et aucun système n'est à l'abri d'une vulnérabilité inconnue. Dans la version 2017 du concours Pwn2Own, deux équipes de hackers ont réussi à exploiter des vulnérabilités inconnues ce qui leur a permis de réaliser une évasion de VM (*VM escape*)[11].

5.3 Niveau de control réduit

En faisant appel à un service d'un fournisseur cloud et quel que soit le modèle, l'utilisation du cloud s'accompagne nécessairement par une perte de contrôle de la part du client. Cette perte de contrôle est maximale lorsqu'on fait appel à un SaaS. Avec cette perte de contrôle, le client peut supposer à tort que seul le fournisseur est responsable de la sécurité du système. On se retrouve alors dans une situation où les mesures des sécurités ne sont pas mises en place par méconnaissance des responsabilités.

5.4 Nouvelle menace interne

Le fournisseur de cloud représente un nouvel acteur dans le système d'information et ses employés sont des sources potentielles de menace interne. Ces employés connaissent bien

[11] https://www.securityweek.com/hackers-earn-200000-vm-escapes-pwn2own-2017

l'infrastructure et ses vulnérabilités et ont généralement un accès privilégié au système et aux données du client.

5.5 Problème de confiance

Faire appel à un service cloud nécessite un minimum de confiance envers le fournisseur cloud qui devient un partenaire pour la gestion et la protection de ces données. Mais peut-on réellement faire confiance à un fournisseur cloud ? Afin d'explorer cette question, il est important de comprendre les intérêts de chaque partie.

5.5.1 Relation client fournisseur

Contrairement à un système d'information classique hébergé en interne, le modèle du cloud introduit une relation commerciale. Le client a intérêt à minimiser les coûts et à mettre en concurrence différents acteurs. Le fournisseur a intérêt à maximiser son gain et à garder le client le plus longtemps que possible. Le fournisseur de services cloud aurait donc tout intérêt à ce que le client soit dépendant de sa solution et pourrait rendre difficile la portabilité du système chez un concurrent.

Il est à noter également que la relation client fournisseur dans le contexte cloud est assez particulière. Les géants du cloud sont dans une position de force et proposent des offres '*as is*' en laissant peu ou pas de marge de négociation aux clients. Il est possible de faire appel à des acteurs cloud moins connus et plus enclin à négocier mais de tels acteurs peuvent généralement se faire racheter voir disparaitre du jour au lendemain.

5.5.2 Risque de concurrence

Amazon a annoncé, fin 2016, le lancement de son service vidéo Amazon Prime. Ce service vient directement concurrencer NetFlix, l'un des plus gros clients d'AWS. Cet exemple montre qu'un fournisseur cloud peut devenir concurrent de son client ce qui peut compliquer les relations entre les deux partie. Si Netflix et Amazon arrivent à bien gérer cette relation et à se partager le marché, cette configuration représente un conflit d'intérêts évident et peut provoquer des tensions entre client et fournisseur.

5.5.3 Fournisseurs soumis à d'autres lois

Certains fournisseurs cloud peuvent être soumis à des lois ou règlementations qui les obligent à communiquer les données qu'ils stockent. Le CLOUD Act, qui a été voté et promulgué aux États-Unis en mars 2018, permet au gouvernement américain de collecter des

données hébergées dans les centres de données des fournisseurs de services cloud Américains même si les données sont en dehors des États-Unis. Il est donc indispensable d'étudier les lois auxquelles les fournisseurs cloud sont soumis afin de juger s'il est convenable de confier telles ou telles données à un hébergeur cloud.

6 Menaces principales dans le cloud et défenses

Le modèle du cloud, malgré son innovation en tant que modèle de consommation de l'IT, repose en grande partie sur des technologies déjà connues et utilisées dans les centres de données traditionnels. Il hérite alors de toutes les vulnérabilités et menaces pouvant affecter le matériel ou le logiciel. Ceci dit, les spécificités du cloud présentent de nouveaux vecteurs de menaces et d'attaques. Il est alors indispensable de protéger le système à la fois contre les menaces classiques et celles spécifiques au cloud.

Les menaces de sécurité étant nombreuses, nous allons nous concentrer sur les 12 plus grandes menaces listées par le CSA (*Cloud Security Alliance*) dans un rapport[12] publié en 2017. Le CSA a recueilli et a compilé différents retours d'expériences d'acteurs du cloud et a réalisé cette liste qui classe les menaces selon leur sévérité.

6.1 Fuite des données

La fuite des données est sans surprise la plus grande menace dans le cloud. Cette menace porte atteinte à la confidentialité, l'un des trois piliers de la sécurité. Une fuite de données consiste à toute divulgation de données confidentielles à des personnes non autorisées. Parmi les données concernées, on peut lister les données à caractère personnel, les données sensibles, les données financières, les propriétés intellectuelles ou les secrets d'entreprises. C'est généralement le crime organisé qui s'intéresse aux données à caractère personnel ou aux données financières. Les concurrents s'intéressent de leur côté plutôt aux données propriétaires et aux secrets d'entreprises.

RedLock, spécialiste de la sécurité dans le cloud, estime dans son rapport de mai 2018[13] que 51% des entreprises ont pu laisser fuiter des données dans le cloud suite à des problèmes de configuration. Ces fuites de données ont des répercussions néfastes sur l'image des entreprises concernées. Les utilisateurs, dont les données ont fuités, subissent un préjudice plus

[12]https://cloudsecurityalliance.org/group/top-threats/#_downloads

[13]https://info.redlock.io/cloud-security-trends-may2018-thank-you?submissionGuid=d06dcf05-aab5-48a5-9a82-47f3c4288344

au moins important et ne font généralement plus confiance à l'entreprise qui a eu la brèche de sécurité.

Equifax, qui héberge des données à caractère personnel dans le cloud, a reconnu en octobre 2017 une fuite des données de 145 millions d'utilisateurs aux États-Unis. Cette faille est due à une négligence de la part d'Equifax qui n'a pas appliqué un patch de sécurité niveau applicatif. Equifax est actuellement poursuivie suite à cette affaire et certains de ses dirigeants ont dû démissionner depuis cet incident.

Si la faille d'Equifax aurait pu être évitée en appliquant le patch au bon moment, il aurait été impossible d'éviter des vulnérabilités non publiées ou sans correctif connu (*Zero Day*). Il est alors essentiel de concevoir une architecture résiliente aux vulnérabilités non connues afin de protéger la confidentialité des données dans le cloud. Les techniques cryptographiques et le contrôle d'accès s'imposent afin d'assurer la confidentialité des données. Nous allons nous intéresser tout au long de cette section à la cryptographie et au chiffrement en particulier et nous allons revenir en plus de détails sur la gestion des accès dans la section 6.2.

Le chiffrement, comme garant de la confidentialité, doit relever deux défis majeurs à savoir la gestion des clés de chiffrement et la capacité à gérer les différents états des données. Les fuites de données impactent en effet les données pendant tout leur cycle de vie. Si les techniques de chiffrement des données au repos ou en transit sont complètement opérationnelles, ce n'est pas le cas des données en utilisation par exemple.

6.1.1 Sécurité des données au repos

Lorsqu'une vulnérabilité ou une attaque expose des données stockées, la confidentialité des données ne doit pas être compromise. Ceci est d'autant plus important pour les données à caractère personnel, les données sensibles ou toutes autres données dont le dévoilement serait préjudiciable à l'organisation ou à ses clients et partenaires. Le chiffrement s'impose alors comme une couche essentielle dans une vision de défense en profondeur afin de garantir la confidentialité de ces données. Le chiffrement, en plus d'être une bonne pratique, peut être obligatoire afin de se conformer à des standards comme le PCI-DSS ou aux règlementations en vigueur comme c'est le cas du RGPD qui exige le chiffrement des données à caractère personnel.

L'algorithme AES est actuellement la référence pour le chiffrement symétrique. Il peut être associé à une clé de 128 bits, 192 bits ou 256 bits. Si un attaquant parvient à récupérer des

données chiffrées en AES sans la clé associé, il lui est quasiment impossible à de déchiffrer les données dans un temps raisonnable avec les puissances de calcul actuelles.

Les fournisseurs de services cloud public proposent quasiment tous des solutions de chiffrement des données au repos. AWS et Azure donnent aux clients la possibilité de choisir entre deux modes de chiffrements (coté serveur et côté client) et plusieurs modes de gestion de clés afin de donner au client le contrôle selon ses exigences en termes de gestion des clés. Google Cloud Platform active le chiffrement des données au repos par défaut et propose également plusieurs modes de gestion de clés en fonction des besoins des différents clients. Il est très important d'analyser les modes de gestion de clé et de choisir celui qui correspond le mieux à la politique de l'organisation et aux exigences de sécurité au regard de la nature des données. Il est vrai qu'une solution de gestion des clés par le fournisseur cloud peut faciliter la vie du client mais il faut être conscient que le fournisseur cloud a accès à toutes les données en clair s'il gère lui-même les clés. La configuration où le fournisseur cloud dispose d'une clé qui lui a été attribuée par le client, en vue d'un traitement particulier, présente également un risque vu que le fournisseur est en mesure de déchiffrer les données. La solution la mieux sécurisée est celle où le fournisseur cloud n'a pas accès aux clés. L'inconvénient majeur d'une telle configuration est l'incapacité du fournisseur d'effectuer des traitements pour le compte de son client. Ceci dit, certaines solutions qui protègent la confidentialité des données en utilisation commencent à voir le jour. C'est ce qu'on va voir dans le paragraphe suivant.

6.1.2 Protection des données en utilisation

C'est quand elles sont en utilisation que les données sont le plus vulnérables. Une application SaaS a besoin de traiter de manipuler des données en clair et c'est à ce niveau que les attaquants vont chercher les vulnérabilités pour attaquer l'application et récupérer des données confidentielles. La protection des données en utilisation est un défi majeur et la recherche n'arrête pas de progresser afin de proposer des solutions dont voici quelques-unes :

- *Chiffrement homomorphe*

Le chiffrement homomorphe est une technique cryptographique qui garantit la confidentialité des données en utilisation. Le sous-traitant, ou le fournisseur cloud, effectue tous les traitements sur des données chiffrées ce qui garantit la confidentialité des données. Seul le client est capable de déchiffrer le résultat du traitement afin d'obtenir le résultat final.

Pour schématiser, le client chiffre le nombre 1 et le nombre 2. Le fournisseur cloud additionne les nombres chiffrés. Par la suite le client déchiffre le résultat de cette addition pour obtenir le nombre 3, donc somme de 1 et 2 :

1 → c85f8f8ea7d3d2b96ab7d2aceb100

\+ = f2318890df523cd5a645221edce3 → 3

2 → d3c05a647df523cd5ae0984af1fc2

Le premier schéma de chiffrement homomorphe complet (*Full Homomorphic Encryption*) a vu le jour en 2009 et il supporte un nombre illimité d'additions et de multiplications dans la même opération. En théorie, ce schéma de chiffrement permet de résoudre le problème de la confidentialité des données et permet une utilisation pour tout type de traitement (Il est possible d'effectuer des opérations AND et XOR au niveau du bit). Si les premières implémentations nécessitaient 30 min pour effectuer un calcul sur 1 bit, la recherche autours des techniques homomorphes avance à grand pas et les performances se sont nettement améliorées même si on reste loin des performances de calcul sur des données non chiffrés :

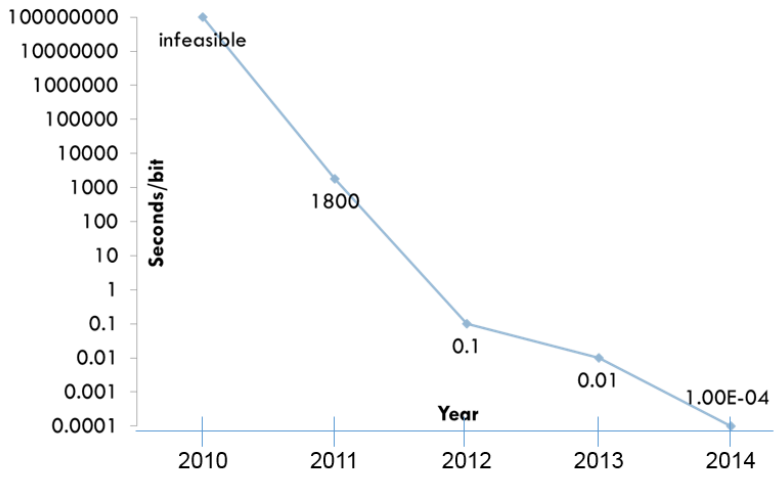

Figure 5 -Performance chiffrement homomorphe[14]

Le chiffrement homomorphe sera surement le graal de la confidentialité des données mais il faudra que la recherche puisse à la fois atteindre des performances acceptables et résoudre certaines faiblesses comme la vulnérabilité face à l'attaque au texte chiffré choisi (*chosen-cypher text attack*)

[14] https://www.maths.ox.ac.uk/system/files/attachments/FHE1.pptx

- *Distribution des données chiffrées*

Malgré leur potentiel énorme en vue de garantir la confidentialité des données traitées, les solutions de chiffrement homomorphe ne sont actuellement pas en mesure d'assurer des temps de réponse satisfaisants. Parmi les alternatives, il existe une approche qui consiste à distribuer les fragments de données sur plusieurs serveurs localisés chez différents fournisseurs (Will, Ko, & Witten, 2016). La confidentialité est garantie par le fait qu'aucun serveur n'est capable de déchiffrer l'ensemble des données distribuées. Une faille de sécurité au niveau d'un serveur ne peut alors pas compromettre la totalité des données.

- *Chiffrement avec recherche par mots clé*

Les données stockées dans le cloud ne font pas toujours l'objet de traitement complexe. Il peut alors être suffisant d'appliquer d'autres techniques de chiffrement qui permettent d'effectuer un traitement précis sur les données chiffrées. De telles solutions sont moins flexibles qu'un chiffrement homomorphe complet mais elles sont beaucoup plus performantes.

Un cas d'utilisation classique consiste à stocker des données chiffrées et de faire une recherche par mot clé. L'utilisation du chiffrement symétrique avec recherche par mot clé (*Searchable Symmetric Encryption*) permet d'effectuer la recherche sur des données chiffrées et garantit une confidentialité par rapport aux données stockées et aux mots clés cherchés.

6.1.3 Sécurité des données en transit

Le recours à une architecture cloud implique des allers-retours de données et il est donc indispensable de sécuriser le flux de données en transit entre le fournisseur et son client. Le protocole TLS s'est largement imposé afin de chiffrer les données en transit dans le réseau. Ce protocole garantie aussi bien la confidentialité que l'intégrité. Il est également possible de mettre en place un VPN en utilisant IpSec, par exemple, ce qui rajoute une couche supplémentaire pour sécuriser le trafic réseau.

6.1.4 Partage sécurisé des données

Le partage des données avec des partenaires ou des sous-traitants est également une grande source de vulnérabilité. Il est essentiel de choisir les entités/personnes avec lesquelles il est possible de partager les données en fonction de la classification de celles-ci. Afin de partager les données de manière sécurisée, il faut mettre en place une bonne gestion d'identité et d'accès et définir les droits et privilèges adéquats pour chaque entité/utilisateur en fonction du besoin. Le principe des **moindres privilèges** doit être respecté. Il n'est pas nécessaire de donner des

droits en écriture par exemple si le partenaire aurait juste besoin de consulter les données. Ceci permet de limiter les dégâts si un compte utilisateur est compromis par exemple.

Hormis l'aspect technique, il ne faut pas omettre l'aspect contractuel lorsqu'il s'agit de partager des données. Les partenaires doivent s'engager afin de mettre en place les mécanismes nécessaires pour la protection des données partagées.

6.1.5 Effacement sécurisé des données

L'effacement sécurisé des données permet de s'assurer que les données effacées sont irrécupérables. Plusieurs techniques d'effacement existent mais elles nécessitent d'avoir accès au stockage physique. Dans le cas du stockage des données chez un fournisseur de services cloud, c'est ce dernier qui se charge d'effacer les données à la demande du client mais il n'y a aucune garantie que les données effacées soient irrécupérables.

Ceci dit, il est possible de faire appel au chiffrement afin de contourner cette problématique dans le cas où le fournisseur ne gère pas les clés. Le principe consiste à chiffrer les données par une clé, puis chiffrer cette clé par une clé de control. On peut supposer que les données sont effacées si cette clé de contrôle est effacée. Cette approche a été proposée comme garantie d'effacement en se basant sur des règles d'accès aux fichiers (Tang, Lee, Lui, & Perlman, 2012). Cette solution est elle-même inspirée d'une autre qui propose une suppression de clé de contrôle après un temps défini choisi au moment du chiffrement (Perlman, 2007)

6.2 Gestion d'identité et d'accès et des identifiants défaillantes

Les techniques cryptographiques vues précédemment présentent un premier pilier essentiel afin d'assurer la confidentialité des données. Le deuxième pilier, non moins important, est la gestion d'identité et d'accès. Ceci consiste à gérer l'identification, l'authentification et l'autorisation des utilisateurs. Les outils en question incluent aussi un système d'enregistrement (*Logging*) afin de tracer des actions des utilisateurs et d'établir les responsabilités. Ces enregistrements peuvent aider les professionnels de sécurité à établir une piste d'audit en cas d'incident de sécurité.

Une gestion d'identité et d'accès et des identifiants défaillantes est une vulnérabilité qui permet à l'utilisateur malveillant d'avoir un accès avec les mêmes privilèges que l'utilisateur légitime. Les dégâts peuvent être énormes selon le degré d'accès obtenu et peut conduire à une fuite ou perte de données ou l'installation de tout type de malware. Avec une porte dérobée par

exemple, l'attaquant peut assurer un accès quasi permanant au système et dispose d'outils afin d'espionner le compte compromis.

En 2017, une étude[15] a révélé que 7% des serveurs S3 d'AWS sont en accès public ce qui expose les données stockées à un risque de perte de confidentialité. C'est ainsi que Fedex a exposé les données privées de milliers de ses clients comme ça a été révélé début 2018. Il y a aussi l'exemple d'Uber qui a eu une fuite de données fin 2016 concernant 600 000 numéros de permis de conduire de ses chauffeurs. Cette fois, c'est le compte Github d'Uber qui s'est fait piraté. Ce compte contenait les identifiants d'accès du compte AWS d'Uber.

Dans ces deux exemples, ce sont les clients d'AWS qui n'ont pas assumé leur responsabilité pour mettre en place une gestion d'identité et d'accès en bonne et due forme. Dans le cas de Fedex, aucune gestion d'accès n'a été mise en place. Dans le cas d'Uber, les identifiants AWS ont été stockés d'une manière non sécurisée dans un service cloud (GitHub). La mise en place d'une authentification multi-facteur aurait réduit le risque.

De telles brèches de sécurité montrent une vraie méconnaissance des bonnes pratiques de sécurité à mettre en œuvre pour la gestion d'identité et d'accès. Tous les grands acteurs de cloud proposent des solutions de gestion d'identité et d'accès mais c'est au client de faire le nécessaire pour gérer les utilisateurs, leurs identifiants et leurs autorisations. Voici une liste de bonnes pratiques recommandées par AWS pour gérer d'une façon sécurisée les identités et les accès :

- **Protection du compte AWS** : AWS préconise de ne pas générer des clés d'accès au compte AWS sauf si c'est indispensable et de privilégier les clés utilisateurs. Il est aussi recommandé d'activer l'authentification multi facteur pour l'accès au compte AWS.
- **Création de comptes utilisateurs** : Il ne faut pas partager les identifiants du compte AWS. L'administrateur doit créer un compte à part pour chaque utilisateur censé avoir accès aux ressources stockées dans le cloud. L'administrateur doit lui aussi passer par un compte utilisateur avec les privilèges administrateur. Les identifiants AWS ne doivent être utilisés que lorsqu'il n'est pas possible de faire autrement. L'administrateur peut attribuer des permissions à chaque utilisateur. Il peut également changer ou révoquer ces permissions selon le besoin.

[15] https://www.bleepingcomputer.com/news/security/7-percent-of-all-amazon-s3-servers-are-exposed-explaining-recent-surge-of-data-leaks/

- **Utilisation des groupes pour les permissions** : AWS recommande de passer par les groupes pour les permissions. Les membres d'un groupe ont des rôles semblables et ont alors besoin d'accéder aux mêmes ressources.
- **Utilisation des politiques AWS pour donner les permissions** : AWS recommande d'utiliser ses politiques de permissions dans la mesure du possible.
- **Respect du principe de moindres privilèges** : Un utilisateur doit disposer juste des privilèges nécessaires afin de pouvoir assumer ses tâches. Cela permet de contenir le risque en cas de compte utilisateur compromis.
- **Vérification des permissions** : La politique de permissions doit être revue régulièrement afin de garantir le respect du principe des moindres privilèges.
- **Mise en place d'une politique de mot de passe** : Il est recommandé d'avoir une politique de mot de passe rigoureuse à savoir : un mot de passe robuste, changement régulier des mots de passe.
- **Mise en place de MFA pour les utilisateurs avec privilèges élevés** : Il est recommandé d'activer l'authentification multi facteur pour les utilisateurs disposant de privilèges élevés.
- **Utilisation des rôles pour les applications** : Le 'rôle' est une entité qui a un ensemble de permissions sans que ça corresponde à un utilisateur ou un groupe. Il est recommandé d'utiliser cette entité pour configurer l'accès des applications à des ressources AWS.
- **Utilisation des rôles pour déléguer les permissions** : AWS déconseille de partager les identifiants pour l'accès à des ressources. Il est alors recommandé d'utiliser les rôles.
- **Rotation des mots de passe** : Il est également recommandé de changer les mots de passe de tous les utilisateurs assez régulièrement afin de limiter la durée d'utilisation d'un compte piraté.
- **Suppression des identifiants inutiles** : Il est recommandé de supprimer tous les identifiants inutiles dans le système, tels que les identifiants d'utilisateurs qui n'ont plus besoin d'accès.
- **Utilisation des règles d'accès** : Il est possible de créer des règles d'accès particulières aux ressources AWS tels que la plage d'IP d'accès ou la plage horaire pendant laquelle il est possible d'accéder aux données.
- **Utilisation des logs pour vérifier l'activité des utilisateurs** : Il est important de vérifier les logs d'accès aux ressources afin de repérer les anomalies. Les logs contiennent l'ensemble des actions avec la date et l'heure de l'action ainsi que l'adresse IP.

6.3 API et interfaces non sécurisées

Les fournisseurs de services cloud proposent à fois des consoles de gestion et des APIs pour tout type d'accès aux ressources. Ces APIs et interfaces permettent au client d'effectuer des tâches standards telles que le provisionnement des ressources mais permettent également d'automatiser les processus et d'orchestrer les différents traitements.

Les APIs sont également la partie la plus exposée du système et elles figurent parmi les cibles préférées des cyberattaquants. Voici les quelques points à considérer afin de sécuriser une API :

- **Sécurité du transport** : Une API ayant accès à des données sensibles doit être appelée en utilisant le protocole TLS. Ceci permet d'assurer la confidentialité et l'intégrité.
- **Authentification** : Une API sécurisée doit pouvoir authentifier tout utilisateur ou application qui essaient d'y accéder.
- **Sécurité des applications** : Les applications qui acceptent les entrées de données de la part des utilisateurs sont exposées à des attaques de type injection SQL. Les entrées de l'API doivent être validées au niveau de l'application. L'OWASP fournit une liste des menaces majeures pour les applications[16]. Il est indispensable que ces menaces soient étudiées et que les développeurs protègent leurs codes contre ces vulnérabilités.

6.4 Vulnérabilités du système

Les vulnérabilités correspondent à tout défaut dans le système que ce soit niveau matériel ou logiciel. TCP/IP présente par exemple des vulnérabilités qui sont dues à son architecture qui n'a pas été pensée pour garantir la sécurité des systèmes d'information. Les vulnérabilités logicielles sont régulièrement dévoilées et des patchs de sécurité sont alors développés afin de corriger les vulnérabilités. Il est indispensable d'effectuer des audits réguliers des vulnérabilités et de s'assurer que les derniers correctifs sont appliqués.

Un système donné peut également avoir des vulnérabilités qui ne sont pas publiquement connues ou sans correctif officiel (*Zero Day*). Il faut être conscient que de telles vulnérabilités peuvent être découvertes et exploitées par des hackers malicieux et ainsi mettre en danger la sécurité du système d'information.

[16] https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

6.5 Piratage de compte

Le piratage de compte est un problème assez courant et connu. Il peut être le résultat d'une gestion défaillante des identifiants, d'une politique permissive de mot de passe ou d'une vulnérabilité applicative. Le cloud ne fait alors que rajouter une nouvelle surface d'attaque. Pirater le compte cloud d'une organisation donne à l'attaquant tous les privilèges afin de compromettre la confidentialité et l'intégrité des données et d'effectuer toute sorte d'actions nuisibles. Les mesures et bonne pratiques vues en 6.1.2 sont alors un premier pas pour réduire le risque de subir une telle menace.

La société Code Spaces a subi en 2014 un piratage[17] de son compte AWS. L'attaque qui s'en est suivi a effacé la plus grosse partie du code source des clients ainsi que le backup associé. La société a dû cesser son activité après cet incident de sécurité. La société aurait pu activer l'authentification multi-facteurs afin de protéger son compte et gérer mieux les backups en les stockant ailleurs que chez AWS.

6.6 Les menaces internes (*Insiders*)

Une menace interne peut provenir de tout employé, ex-employé, prestataire ou autre partenaire qui dispose des autorisations pour accéder au réseau et aux données de l'entreprise et qui intentionnellement ou pas utilise son accès privilégié pour compromettre la sécurité des données et du système d'information.

Dans un contexte cloud, les employés du fournisseur cloud sont potentiellement de nouvelles sources de menaces internes. Plus le contrôle du fournisseur de services est élevé (en SaaS par exemple), plus la menace est élevée. Les solutions de chiffrement dont on a parlé précédemment sont vulnérables à ces menaces internes si le client confie au fournisseur la gestion des clés de chiffrement. Afin de minimiser le risque de menace interne provenant du fournisseur de services cloud, le client doit d'assurer que son fournisseur met en place certaines bonnes pratiques :

- Le fournisseur de services cloud doit respecter le principe séparation des responsabilités afin d'éviter qu'un employé malintentionné puisse avoir la main et compromettre un processus complet.
- Le fournisseur de services cloud doit respecter le principe des moindres privilèges.

[17]https://www.cloudcomputing-news.net/news/2014/jun/19/code-spaces-rip-code-hosting-provider-ceases-trading-after-well-orchestrated-ddos-attack/

- Le fournisseur de services cloud doit mettre en place un système d'enregistrement d'activité qui permet d'auditer les activités d'administration.

6.7 Menaces persistantes avancées

Les menaces persistantes avancées (*Advanced Persistent Threats*) sont des attaques qui visent à s'introduire dans un système dans le but de s'installer durablement. Ces attaques ciblent généralement les grands groupes ou les gouvernements et ont comme objectif d'obtenir des données confidentielles ou propriétaires. Ces attaques sont lancées discrètement par des acteurs qui ont beaucoup de moyens et qui vont donc user de tous les moyens possibles pour arriver à leurs fins. Ces attaques sont difficiles à détecter et à éliminer.

Ceci dit une bonne part des vulnérabilités à l'origine des APTs sont humaines. Il est alors indispensable de former les utilisateurs afin qu'ils aient conscience des dangers des techniques d'ingénierie sociale ou de l'exécution d'un fichier venant d'une source non fiable par exemple. Les services informatiques doivent également être informés des dernières attaques afin de de s'en protéger.

6.8 Perte de données

La disponibilité des données dans le cloud a toujours été un argument de vente pour les fournisseurs de services cloud. Plusieurs clients vont alors dans le cloud afin d'éviter la perte de leurs données. Ceci dit, les données stockées dans le cloud peuvent être perdus pour diverses raisons. Il y a bien entendu les cyberattaques comme celle subi par Code Spaces mais cette perte de données peut être causée accidentellement par le fournisseur ou être le résultat d'une catastrophe naturelle ou un feu.

Il est alors de la responsabilité du client de :

- vérifier la politique de backup du fournisseur et vérifier si elle est conforme aux attentes et besoins de l'organisation ;
- vérifier les mesures de réplications des données critiques au business ;
- vérifier que le fournisseur cloud suit les bonnes pratiques en termes de plan de continuité d'activité ;
- envisager, selon la criticité des données, de gérer certains backups en interne en plus des backups gérés par le fournisseur cloud. Ceci permet de minimiser le risque de perte de données.

6.9 Manque de vérification et de réflexion autour du cloud

Comme vu précédemment, l'adoption de technologies cloud doit s'inscrire dans une stratégie globale et demande beaucoup d'effort afin de bien se préparer et comprendre les risques encourus. Vouloir aller trop vite vers le cloud, et négliger ces étapes clés, peut mettre l'organisation dans une position difficile.

Il est alors nécessaire d'analyser et de comprendre les spécificités des architectures basées sur le cloud afin d'éviter les problèmes de conception. Il faut également bien étudier la question de la sécurité des données dans le cloud et réaliser toute la phase d'analyse des risques.

Quand la transition vers le cloud est décidée, il faut choisir les services et les fournisseurs cloud qui répondent aux besoins de l'organisation en termes de fonctionnalités, de sécurité et de conformité légale. Le client doit alors bien analyser les SLAs des différents fournisseurs et les croiser avec ses exigences.

6.10 Utilisation malicieuse des services cloud

Les infrastructures cloud sont souvent victimes de différentes cyberattaques mais elles peuvent également servir à des acteurs malicieux de ressources pour lancer des attaques. Les fournisseurs de services cloud n'exigent généralement qu'une carte bancaire afin de vendre leurs services à un client. Ce dernier, s'il est malicieux, peut utiliser une carte piratée afin d'accéder à des ressources cloud et lancer différents types d'attaques. Les cybercriminels peuvent également utiliser les vulnérabilités du système afin de compromettre un compte cloud et l'utiliser à des fins criminelles. Ça a été le cas du service EC2 d'AWS qui, en 2009, a été utilisé comme '*Command And Control*' pour le Botnet Zeus[18].

Ce type d'utilisation du cloud peut avoir des répercussions sur les performances générales. Les ressources sont allouées pour participer à une cyberattaque au lieu de servir des utilisateurs légitimes. C'est au fournisseur cloud de mettre en place les mécanismes nécessaires afin de détecter les paiements frauduleux et tout type d'utilisation abusive des services cloud.

6.11 Déni de service (DoS)

Un déni de service DoS a lieu lorsque les données ou les applications sont inaccessibles à l'utilisateur quand ce dernier tente d'y accéder. Le déni de service porte atteinte à la disponibilité, troisième élément de la triade CIA. Le déni de service peut être le résultat d'une

[18] https://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/

attaque qui cible à exploiter une vulnérabilité d'un système donné mais il peut également se produire lorsque le système est utilisé dans des conditions qui mettent en évidence cette vulnérabilité. Un site internet peut par exemple subir un déni de service pendant la période des soldes suite à grand nombre de clients qui essaient de se connecter. Dans ce cas, c'est l'incapacité du système à monter en charge qui crée l'effet DoS. Lorsqu'il s'agit d'une attaque, le cybercriminel essaie généralement d'exploiter des vulnérabilités à différents niveaux protocolaires. Les attaques procèdent généralement en allouant énormément de ressources pour saturer le système et faire en sorte qu'un nouvel utilisateur ne puisse pas y avoir accès.

On parle également de DDoS (*Distributed Denial of Service*) quand l'attaque provient de plusieurs sources en même temps. Les DDoS amplifient l'effet d'une attaque DoS par le nombre de sources qui lancent cette attaque. Une étude[19] révèle qu'une bonne partie des attaques DDoS servent d'écran de fumée pour distraire les équipes de défense IT et permet ainsi aux cyberattaquants pour lancer des attaques plus dangereuses. Il est indispensable alors de doubler d'attention non seulement pour arrêter l'attaque DDoS mais également pour protéger les systèmes contres d'éventuelles attaques plus pernicieuses.

Si les attaques DoS ne sont pas spécifiques au cloud, les infrastructures et les applications cloud souffrent beaucoup de ces attaques. Une étude[20] sur la sécurité des infrastructures révèle que :

- 61 % des opérateurs de centres de données ou cloud ont enregistré en 2016 des attaques ayant entièrement saturé leur bande passante ;
- 21 % de ces opérateurs ont subi plus de 50 attaques DDoS par mois.

Les conséquences de telles attaques peuvent être importantes. On distingue les conséquences d'ordre financier et ceux affectant la réputation de la victime. Un site e-commerce qui subit une attaque DoS quelques jours avant les fêtes, période où il réalise une bonne partie de son chiffre d'affaire, peut subir d'énormes pertes financières selon la durée d'indisponibilité du site en question. La réputation peut également être affectée et le client peut perdre confiance et aller voir la concurrence.

Il n'y pas de système standard pour se protéger contre les attaques de type DoS vu les différents modes opératoires. Les solutions anti-DoS intégrés niveau Firewall ou au niveau des IDS sont toujours utiles mais d'autres solutions plus efficaces existent comme les solutions de

[19] https://www.kaspersky.com/about/press-releases/2016_research-reveals-hacker-tactics-cybercriminals-use-ddos-as-smokescreen-for-other-attacks-on-business

[20] NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report

nettoyage DDoS[21] (DDoS *scrubbing solution*). Akamai propose une solution de ce type et déclare avoir stoppé une attaque[22] à 1,3 Tbit/s à l'aide de son système.

6.12 Vulnérabilités liées au partage des ressources

Si les architectures multi-tenant qui caractérisent le cloud permettent une meilleure mutualisation des ressources, elles représentent aussi un risque en termes de sécurité. Dans un service IaaS, ce partage de ressource est surtout réalisé à l'aide de la virtualisation. Dans un contexte SaaS, ce partage provient du fait que tous les utilisateurs ont accès à la même application.

Voici une liste des risques[23] les plus importants liés au partage des ressources :

- une séparation logique inadaptée,
- des utilisateurs malintentionnés ou négligents,
- des ressources partagées qui sont des points de panne unique (*Single Point of Failure*),
- une gestion de configuration défaillante,
- des données de plusieurs utilisateurs mélangées,
- des problèmes de performances,
- des risques spécifiques :
    - IaaS : attaques Cross VM,
    - PaaS : vulnérabilités liés à la plateforme,
    - SaaS : gestion des données, back-up, archives dans les mêmes bases de données.

Si certaines mesures sont de la responsabilité des fournisseurs cloud, ces derniers sont parfois assez vagues sur leurs architectures ou les mesures de sécurité en place. Le client doit être conscient du risque qu'il prend et doit adopter une approche de défense en profondeur afin de réduire le risque. Il doit alors faire appel au chiffrement quand c'est nécessaire et mettre en place une bonne gestion de l'identité et d'accès.

[21] Ponemon – The cost of Denial-of-services attacks
[22] https://www.akamai.com/fr/fr/products/cloud-security/ddos-protection-service.jsp
[23] https://www.owasp.org/index.php/Cloud-10_Multi_Tenancy_and_Physical_Security

7 Le RGPD

Comme vu précédemment, la fuite des données est la première menace dans un contexte cloud. La protection de la confidentialité et de l'intégrité des données est alors un enjeu majeur afin de sécuriser un système d'information qui fait recours à des services cloud. Cette protection n'est pas uniquement une question business ou d'image. Elle est également une obligation légale notamment lorsqu'il s'agit de données à caractère personnel ou sensibles. Les entreprises qu'elles soient dans une position de fournisseur ou de client doivent respecter les différentes lois auxquelles elles sont soumises. La nature même du cloud rend cette tâche difficile vu que le client perd le contrôle sur la localisation des données et doit en quelque sorte faire confiance à son fournisseur. Un autre problème est celui du modèle d'affaires (*business model*) cloud qui se base sur les offres d'adhésion et qui donne alors trop peu de marge aux entreprises afin de négocier leurs contrats avec les fournisseurs de services cloud. La directive européenne 95/46/CE était la référence en matière de protection des données à caractère personnel mais elle n'était pas très adaptée au modèle du cloud. Les fournisseurs de cloud sont en effet souvent basés en dehors de l'union européenne et les amandes en cas de manquement ne dissuadaient pas les géants du cloud pour qui les sommes en jeu étaient dérisoires. Le RGPD, entré en application le 25 mai 2018, est le nouveau texte en vigueur. Il a comme principal objectif de protéger les données à caractère personnel des résidents de l'Union Européenne. Ce règlement a adressé certains faiblesses de l'ancienne directive et ceci à travers les points suivants :

- Contrairement à la directive 95/46/CE, le RGPD est un règlement donc un acte juridique applicable directement sans avoir besoin de lois nationales.
- L'extraterritorialité du RGPD fait en sorte que toute entreprise qui traite des données de résidents européens est soumise à ce règlement.
- Les amendes peuvent aller jusqu'à 4% du chiffre d'affaire pour les entreprises ou 20 millions euros.

Se conformer à ce texte est un vrai défi pour toutes les entreprises qui sont soumis au RGPD. Nous allons alors essayer de préciser le champ d'application du RGPD ainsi que les obligations qui en découlent.

7.1 Champ d'application

Le RGPD s'applique du moment que l'entreprise participe à la collecte, stockage ou traitement de données à caractère personnel. Il concerne aussi bien les entreprises établies en Union Européenne que celles qui offrent des services et des biens à des résidents de l'union

indépendamment du lieu d'établissement. Il est alors rare qu'une entreprise se retrouve en dehors du cadre du RGPD. Ceci est d'autant plus vrai pour les entreprises faisant appel aux services cloud et qui placent généralement les données au centre de leur stratégie. Les fournisseurs de services cloud sont bien évidemment tous concernés également et ceci quel que soit leur lieu d'établissement.

7.2 Rôles et responsabilités

Le RGPD, dont le but est de protéger les personnes concernées par un traitement, fait apparaitre deux autres rôles : Celui de responsable de traitement et celui de sous-traitant. Les deux ont des responsabilités et des obligations afin de garantir la sécurité des données à caractère personnel.

Si on prend l'exemple d'une entreprise X qui fait de la vente en ligne et qui fait appel au service d'une entreprise Y pour la gestion du site e-commerce, on peut considérer que les clients du site sont les personnes concernées par le traitement, que l'entreprise X est le responsable de traitement et que l'entreprise Y a le rôle de sous-traitant.

7.2.1 Le responsable de traitement

Le responsable de traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement » (article 4.7)

Le responsable du traitement est le premier responsable de la sécurité des données à caractère personnel. C'est à lui de veiller à la protection des données dès la conception et à leur protection par défaut.

Voici, entre autres, ses obligations afin d'assurer cette sécurité des données :

- Selon l'article 24.1 « le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement ».
- Selon l'article 28.1, le responsable de traitement ne fait appel qu'à des sous-traitants capables de mettre en place les mesures nécessaires pour la protection des données à caractère personnel.

7.2.2 Le sous-traitant

Le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement » (article 4.7)

Dans un contexte cloud, **le sous-traitant est le fournisseur de services cloud** auquel un client fait appel pour utiliser un service donné.

En France, et avant l'entrée en vigueur du RGPD, seul le responsable de traitement était soumis à la loi informatique et liberté. Les obligations du sous-traitant figuraient dans le contrat qui le liait au responsable du traitement. Le RGPD vient alors renforcer la responsabilité du sous-traitant qui est censé alors être proactif et œuvrer pour la sécurité des données.

Voici les obligations majeures du sous-traitant introduites par le RGPD :

- Le sous-traitant doit rédiger avec son client un contrat ou tout acte juridique qui détaille les obligations de chaque partie selon les dispositions de l'article 28.3. Il s'engage par exemple à ne traiter que « les données à caractère personnel que sur instruction documentée du responsable du traitement » et il « veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité. »
- Le sous-traitant doit obtenir l'accord du responsable du traitement s'il souhaite faire appel lui-même à un sous-traitant (article 28.2).
- Le sous-traitant doit informer son client (le responsable de traitement) s'il pense qu'une de ses instructions constitue une violation de la sécurité des données. Il est également dans un rôle de conseil et doit faire son possible pour aider son client à se confirmer au RGPD.

7.3 Mise en place de la conformité au RGPD

La CNIL propose un ensemble d'actions[24] afin de se conformer au RGPD.

[24] https://www.cnil.fr/fr/rgpd-par-ou-commencer

- *Constitution d'un registre de traitement des données*

Selon les dispositions de l'article 30, il est obligatoire à la fois pour le responsable de traitement et pour son sous-traitant de tenir un registre des activités de traitement des données. Ce registre a pour objectif de recenser pour chaque activité l'ensemble des éléments suivants :

- la finalité ou l'objectif du traitement,
- les données utilisées pour le traitement,
- les parties (personnes, services, partenaires…) autorisées à accéder aux données,
- la durée de conservation des données.

- *Tri des données*

Durant cette étape et en lumière du registre du traitement, il est question de vérifier les points suivants :

- Seules les données nécessaires sont utilisées pour les traitements.
- Les données sensibles ne sont pas traitées (sauf exception[25]).
- Seules les personnes habilitées ont accès aux données en cas de besoin.
- Les données ne sont pas conservées au-delàs de la durée nécessaire.

- *Respect des droits des personnes*

Le RGPD vient renforcer l'obligation de transparence vis-à-vis de l'utilisateur qui fait l'objet d'une collecte de données. L'utilisateur a alors le droit aux informations suivantes qui doivent figurer clairement au niveau du support de collecte (Article 13) :

- la finalité de la collecte de données,
- le fondement juridique de cette collecte,
- les parties autorisées à accéder aux données,
- la durée de conservation des données,
- les modalités pour que les personnes puissent exercer leurs droits,
- les pays destinataires et le cadre juridique en cas de transfert hors Union Européenne.

L'utilisateur dispose aussi d'une série de droits que le responsable de traitement et le sous-traitant doivent respecter :

- Article 16 : le droit de rectification ;
- Article 17 : le droit à l'effacement (droit à l'oubli) ;
- Article 18 : le droit à la limitation du traitement ;

[25] https://www.cnil.fr/fr/cnil-direct/question/495

- Article 19 : l'obligation de notification concernant la rectification, l'effacement de données ou limitation du traitement ;
- Article 20 : le droit à la portabilité des données.

➢ *Sécurité des données*

Selon l'article 32, le responsable de traitement et le sous-traitant doivent mettre en œuvre les mesures nécessaires afin de garantir la sécurité des données à caractère personnel et ceci selon la criticité des données en question.

Il est aussi obligatoire de conduire une analyse d'impact relative à la protection des données lorsqu'un traitement « est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques » (article 35). Le but est de trouver les mesures de sécurité adéquates en fonction du niveau du risque.

En cas de violation de de données à caractère personnel, il est obligatoire de notifier l'autorité de contrôle à savoir la CNIL pour la France. (Article 33)

7.4 Limites du RGPD

Comme évoqué en 5.5.3, certains fournisseurs cloud peuvent être soumis à des lois qui les obligent à violer la confidentialité des données de résidents européens. Le CLOUD Act oblige ainsi les acteurs de cloud américains à divulguer des données hébergés indépendamment de la localisation des données. Sachant que les États-Unis n'ont conclu, à ce jour, aucun accord avec l'Union Européenne, le CLOUD Act est alors en totale contradiction avec l'article 48 du RGPD, qui stipule qu'aucune décision d'une autorité administrative d'un pays tiers pour divulgation de données à caractère personnel «ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international ». Selon la nature des données en question, ce type de problématique doit être également pris en compte avant toute décision et choix de fournisseur.

Même si le RGPD présente une avancée pour la protection des données à caractère personnel, il n'a pas vocation à gérer tous les aspects de la relation client fournisseur cloud. Le RGPD est assez explicite, par exemple, sur le droit à portabilité des données à caractère personnel mais il est assez discret par rapport à la réversibilité d'autres données confiées par l'entreprise à un fournisseur cloud dans un cadre de sous-traitance. Il est alors indispensable de prévoir des clauses supplémentaires afin que le client puisse se protéger contre certains risques spécifiques.

8 Le contrat cloud

L'aspect contractuel est extrêmement important afin de gérer la relation client fournisseur inhérente au modèle du cloud. Contrairement au cloud privé, qui donne la possibilité de négocier un contrat, les offres de cloud public que ce soit en IaaS ou en SaaS sont généralement des offres d'adhésion et il n'est pas à la portée de tous de négocier avec les géants du cloud. Ces derniers ont une forte culture du produit et de la mutualisation des ressources et ils ont fait le choix d'éviter tout sur mesure quitte à perdre certains clients ayant des besoins spécifiques. Les quelques clients qui arrivent à négocier ont généralement un poids financier assez conséquent en terme d'activité cloud.

Avec le RGPD, le rapport de force s'équilibre un peu. Cette règlementation, à travers son article 28-3, liste les éléments qui doivent figurer dans un contrat cloud afin de protéger les données à caractère personnel. Le contrat prévoit alors que le fournisseur cloud :

- « ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement… » ;
- « veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité… » ;
- prend toutes les mesures pour assurer la sécurité des données à caractère personnel ;
- ne fait pas appel à un sous-traitant sans accord de responsable du traitement ;
- « tient compte de la nature du traitement, aide le responsable du traitement... » ;
- « selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation… » ;
- « met à la disposition du responsable du traitement toutes les informations nécessaires pour apporter la preuve du respect des obligations …» ;

Ceci dit le RGPD ne règle malheureusement pas tous les problèmes comme vu précédemment. Il est essentiel alors de prévoir une **clause de réversibilité** afin de gérer proprement la fin du contrat. L'entreprise si elle est en position de négocier, peut essayer également de mettre en place des pénalités en cas de non-respect de SLA vue que les compensations proposées par les fournisseurs cloud sont généralement dérisoires et complètement dé-corrélées du préjudice client.

9 Conclusion

Si le cloud représente de nouvelles opportunités et avantages pour les organisations, il est également un nouveau vecteur de vulnérabilités que différents acteurs ont déjà commencé à exploiter à des fins diverses et variées. Une bonne partie des failles de sécurité enregistrées les dernières années est due à une grande méconnaissance du cloud, de ses spécificités et des responsabilités des différents acteurs. Certains pensent, à tort, que le modèle du cloud dégage l'entreprise de toute responsabilité et de tout effort. La réalité est toute autre avec un modèle qui implique une vraie responsabilité du client et la nécessité d'avoir des ressources dédiés aux aspects cloud. Il faut également repenser la sécurité afin qu'elle s'adapte à la disparition du périmètre de l'entreprise et bâtir une nouvelle sécurité centrée sur la protection des données. Si certaines solutions techniques, tels que le chiffrement et la gestion d'identités et d'accès, permettent d'améliorer la sécurité dans le cloud, il est indispensable d'effectuer une vraie analyse des risques afin de mettre en place les défenses appropriées selon la criticité du risque à mitiger. Même si le cadre juridique a pris du retard sur le sujet, le RGPD est un grand pas en avance pour renforcer la responsabilité des fournisseurs cloud dans la protection des données. Ceci dit, ni les mesures techniques, ni le RGPD ne sont capables d'assurer et de garantir une relation de confiance entre client et fournisseur cloud. Les scandales, comme celui de la NSA, nous ont démontré que nous ne pouvons pas compter sur les lois et les accords internationaux afin d'avoir un rapport transparent avec les fournisseurs cloud. Paradoxalement, les acteurs les plus fiables en termes de sécurité et les plus innovants en termes de services sont les géants du cloud américains qui suscitent pas mal d'inquiétudes. L'arrivé des géants chinois du cloud n'arrangera surement pas le problème. Il est alors légitime de se poser des questions sur le modèle actuel du cloud. Ce modèle implique une certaine dépendance vis-à-vis du fournisseur et une perte de contrôle de la part du client qui n'a d'autre choix que faire confiance. Il convient alors de se tourner vers les solutions technologiques basées sur la cryptographie afin de relever ce défi. La technologie Blockchain, qui a démontré son efficacité pour décentraliser les échanges, pourrait peut-être contribuer à bâtir le cloud du futur qui sera distribué, décentralisé et basé sur notre confiance envers la technologie!

Bibliographie

Cloud Computing BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY - ENISA

http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

https://www.secureworldexpo.com/industry-news/attacks-on-cloud-2017

https://www.veritas.com/form/whitepaper/the-truth-in-cloud

https://www.nist.gov/publications/cloud-computing-security-foundations-and-challenges-chapter-14-cloud-computing-security

https://www.salesforce.com/products/platform/products/shield/

https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v%3dcs.20)

http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees

https://focus.forsythe.com/articles/619/7-Steps-to-Effective-Data-Classification

https://www.securityweek.com/hackers-earn-200000-vm-escapes-pwn2own-2017

https://cloudsecurityalliance.org/group/top-threats/#_downloads

https://info.redlock.io/cloud-security-trends-may2018-thank-you?submissionGuid=d06dcf05-aab5-48a5-9a82-47f3c4288344

https://www.maths.ox.ac.uk/system/files/attachments/FHE1.pptx

https://www.bleepingcomputer.com/news/security/7-percent-of-all-amazon-s3-servers-are-exposed-explaining-recent-surge-of-data-leaks/

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

https://www.cloudcomputing-news.net/news/2014/jun/19/code-spaces-rip-code-hosting-provider-ceases-trading-after-well-orchestrated-ddos-attack/

https://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/

https://www.kaspersky.com/about/press-releases/2016_research-reveals-hacker-tactics-cybercriminals-use-ddos-as-smokescreen-for-other-attacks-on-business

https://www.akamai.com/fr/fr/products/cloud-security/ddos-protection-service.jsp

https://www.owasp.org/index.php/Cloud-10_Multi_Tenancy_and_Physical_Security

https://www.cnil.fr/fr/rgpd-par-ou-commencer

https://www.cnil.fr/fr/cnil-direct/question/495

NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report

Perlman, R. (2007). File System Design with Assured Delete. *ISOC NDSS*.

Ponemon – The cost of Denial-of-services attacks

Tang, Y., Lee, P. P., Lui, J. C., & Perlman, R. (2012). FADE: Secure Overlay Cloud Storage with File. *IEEE Transactions on Dependable and Secure Computing*, 903–916.

Will, M. A., Ko, R. K., & Witten, I. H. (2016). Privacy Preserving Computation by Fragmenting Individual Bits and Distributing Gates. *IEEE TrustCom/BigDataSE/ISPA*.

Glossaire

AES : Advanced Encryption Standard

API : Application Programming Interface

APT : Advanced Persistent Threats

AWS : Amazon Web Services

CIA : Confidentiality, Integrity, Availability

CLOUD Act : Clarifying Lawful Overseas Use of Data Act

CNIL : Commission nationale de l'informatique et des libertés

CSA : Cloud Security Alliance

DDoS : Distributed Denial of Service

DLP : Data Loss Prevention

DoS : Denial of Service

ENISA : European Union Agency for Network and Information Security

IaaS : Infrastructure as a Service

IP : Internet Protocol

IT : Information Technology

MFA : Multi-Factor Authentication

NIST : National Institute of Standards and Technology

NSA : National Security Agency

OWASP : Open Web Application Security Project

PaaS : Platform as a Service

PCI-DSS : Payment Card Industry Data Security Standard

PME : Petites et Moyennes Entreprises

RGPD : Règlement Général sur la Protection des Données

SaaS : Software as a Service

SI : Système d'Information

SLA : Service-Level Agreement

TCP : Transmission Control Protocol

TLS : Transport Layer Security

VM : Virtual Machine

VPN : Virtual Private Network