Introduction

Cloud Computing et IOT

M2I 3 ème année

Guillaume PETIT

Sommaire :

Introduction :

Définition du cloud computing, d'après le NIST (équivalent à l'ANSSII aux USA) :

- Modèle omniprésent,
- Adapté aux besoins,
- Disponible à la demande,
- Utilise des réseaux accéder à des moyens informatiques (partagés et confidentielles),
- Les moyens informatiques peuvent être libéré en fonction des besoins (avec un effort minimal de configuration),

Un hébergeur de cloud à plusieurs data center repartis sur différents pays.

Au sein du cloud, la facturation est assez spécifique elle est basée sur la télémétrie d'utilisation, la télémétrie peut ce basée sur :

- Le temps d'utilisation,
- Le transfert de données,

Il ne faut pas que la raison de passer dans le cloud soit purement économique.
Il faut qu'un expert de la cyber sécurité soit conscient de cœur de métier de leur entreprise.

Raison de passer dans le cloud :

- Economique l'informatique c'est un coût et ça ne rapporte rien,
- Externaliser ses données pour un gain de sécurité,

Migration du SI dans le cloud :

La sécurité du SI est dictée par la réalité économique, Il faut d'abord modéliser tous les processus d'une entreprise. Passer dans le cloud implique un changement de travail.

Migration dans le cloud, assessment :

- 1 Recenser tous les processus de l'entreprise -> BPL (Business Process Language),
- 2 Recenser tous les biens,
- 3 Recenser tous les besoins,

Inventaire matériel et logiciel :

a) Echanger avec les cadres (lister les biens, les besoins),
b) Echanger avec les salariés,
c) Echanger avec les clients,
d) Volumétrie moyenne du réseaux (séparer les flux),
e) Inventaire logiciel /matériel,
f) Inventaire des données comptables,
g) Inventaire des assurances, qu'est qui se passe si on déplace les data dans le cloud ?
h) Inventaire des données personnelle,
i) Analyser impact juridique (RGPD recommande que cette information soit à un seul endroit et pas d'autres),

La phase d'assessment est terminé.

BIA : Business Impact Analysis, Etude d'impact sur la productivité de l'entreprise si un processus métier ou un équipement / bien sur lequel repose le processus à faillir

Etablir les chemins critiques : Les processus que l'on ne pourra pas interrompre,
Evaluer l'impacte économique en cas de rupture du process,

L'analyse de tous les processus qui ont un impact critique sur l'entreprise. Evaluer le coût de mise en conformité.

Ce sont uniquement les chemins critiques qu'il faut externaliser dans le cloud.

Il est recommandé de faire intervenir un spécialiste :

- Etablir les chemins critiques les processus que l'on ne pourra pas interrompre,
- Evaluer l'impact économique en cas de rupture du processus,
- Evaluer coût de mise en conformité,
- L'informatique rentre en jeu ici,

Cloud -> Réduction des coûts :

- Réduction de la masse salariale,
- Réduction coût des opérations (contrat de maintenance, changer le hardware),
- Réduction des couts de mis en conformité (RGPD, ISO 270001),

-

Il y a du vrai mais c'est une vision dangereuse, mais ce ne doit pas être la raison principale.

La raison principale :
Ce sont uniquement les chemins critiques qu'il faut externaliser dans le cloud.

Le personnel dans le BIA considère l'humain comme un "bien".

Les risques du cloud :

- Mauvaise transition,
- On va faire disparaître des risques mais on va en faire apporter de nouveaux,
- La récupération des données,

Ne jamais foncer tête baisé dans un projet du cloud.

Modèle de cloud :

3 Grand modèle de cloud :

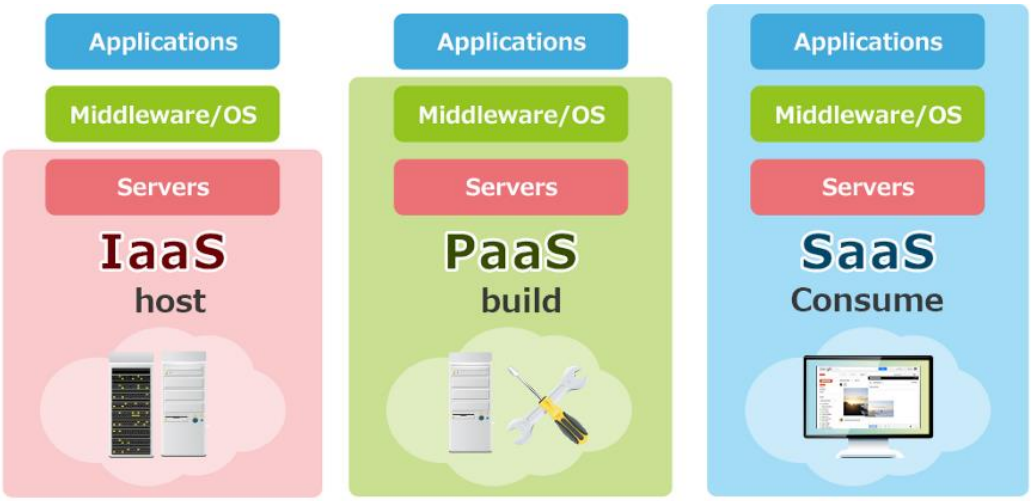

Illustration 1 : *Type de modèle de cloud.*

- SaaS : **Software as a Service**, exemple email, Outlook, CRM, le cloud s'occupe de tout,
  - - Perte de compétence en interne
  - - Patrioct Act

- PaaS : **Plateform as a Service** (système d'exploitation on gère tous le serveur mais les mises à jours) C'est IaaS plus install et maj des OS et quelques fois avec un hardening des OS. Ont peut pas tout changer dans cet OS
  - + devops
  - - manque de visibilité sur le hardening
  - - difficulté à modifier paramètres bloqués

- IaaS : **Infra as a Service**, serveur nu complètement nu ou on a tout dessus on arrive il faut installer l'OS, garantie par le cloud intégrité matériel et accès réseau On s'epargne juste les serveurs dans nos locaux
  - + On garde la main sur la sécurité
  - + Très utilisé pour la sauvegarde de données
  - + Très utilisé pour le PRA / PCA
  - + Grande disponibilité
  - - Toujours de l'administration à faire
  - - Mises à jour à faire
  - Le gain cloud est minime

Outil utilisé par netflix pour produire des pannes au sein de leur infra :

- Chaos Monkey
- Doctor Monkey
- Lattency Monkey

Simian Army ils sont là pour foutre le bordel dans les T4 de netflix source du code : https://github.com/Netflix/security_monkey

Au-delà de la capacité du datacenter il faut que les équipes soit opérationnel l'outil de Netflix permet d'entrainement.

Modèle de déploiement :

Les modèles de déploiements :

- Cloud public : possédés par le fournisseur partager entre tous les clients (ex AWS)
- Cloud privé : l'infra d'une entreprise,
  - Réseau dédié,
  - Service soit accessible depuis l'extérieur (VPN, DMZ, frontal)
  - Ne sert qu'à l'entreprise
  - **Pas forcément dans les locaux**
- Cloud communautaire Ce sont des entreprises qui se regroupe pour former un cloud commun
  - Associations
  - Personnes privée https://owncloud.com
- Hybride : mix public / privé / communautaire

Type de datacenter :

Les types de datacenters :

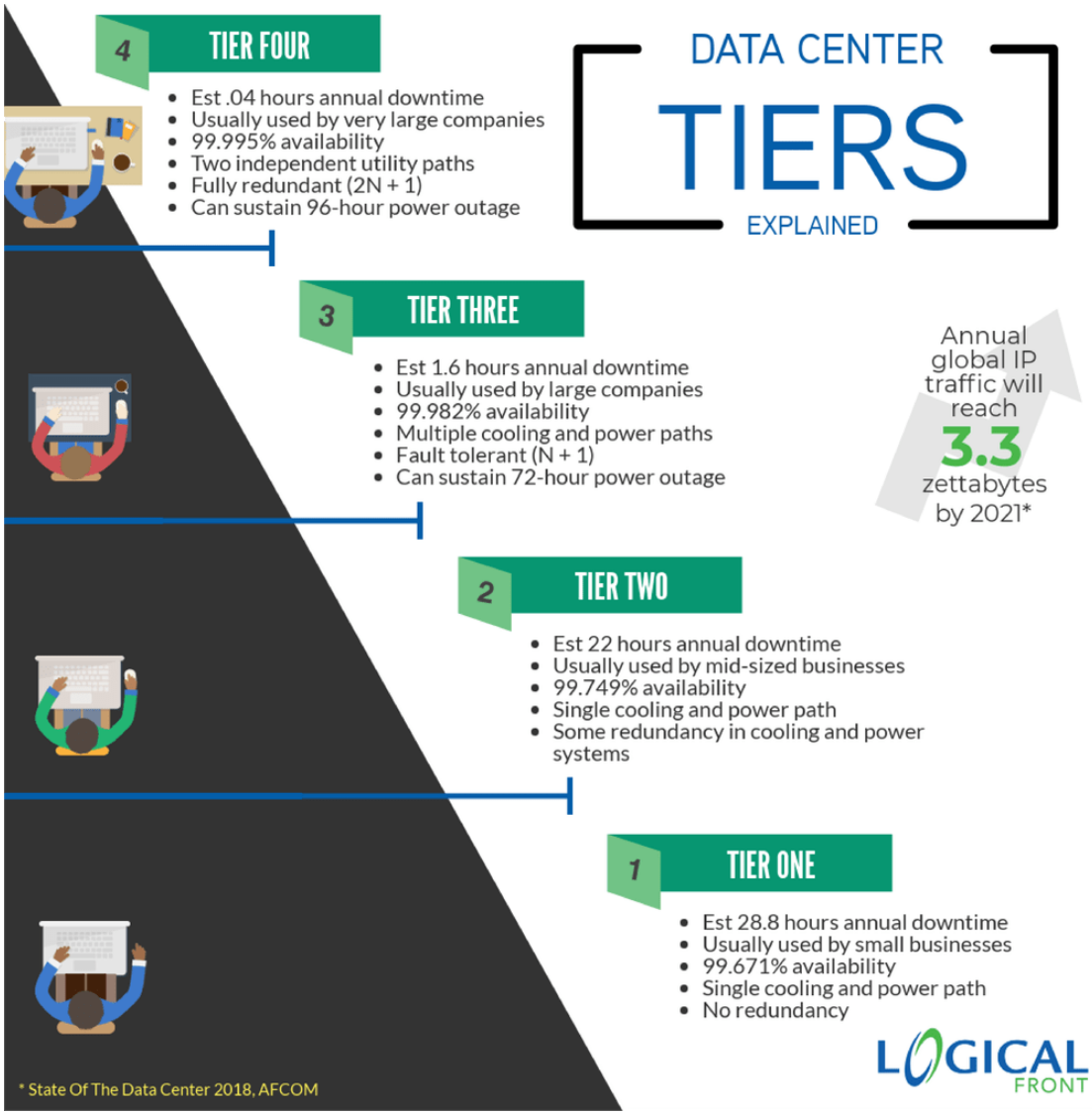

Illustration 2 : *Les niveaux de cloud.*

- T1 : **Le moins cher peu de redondance -> interruption de service**
  - Alimentation de secours pour serveur et sauvegarde (onduleurs)
  - Coupures plus longue générateur électrique tenant jusqu'à 12H
  - Système spécifique de refroidissement des systèmes critiques
  - Espace dédié aux serveurs,
  - Espace dédié aux réseaux,
  - Une erreur de manipulation cause une interruption de service

- T2 : T1 amélioré, plus de résilience
  - Redondance des serveurs et du réseau
  - Erreur de manipulation l'arrêt du service n'est pas systématique
  - En cas de maintenance planifiée pas de coupure de service,

- En cas de maintenance non planifiée des coupures de services possible

- T3 = T2 amélioré
  - Tous les équipements électroniques ont un système d'alimentation électrique redondant,
  - L'opération essentielle continue en cas de panne d'un composant,
  - Les opérations non essentielles peuvent continuer en cas de panne mais ce n'est pas systématique,
  - Un système en panne s'éteint,

- T4 = T3 amélioré (dans PACA jaguar network c'est le seul)
  - Tout est redonnant
  - La panne d'un système n'a pas de conséquence sur un service,
  - Les erreurs de manipulations ne causent pas d'arrêt de service
  - L'évolution technique ne cause pas d'arrêt technique,

Mener un inventaire :

Au niveau cyber il faut connaitrez l'ensemble des processus qui sont migrer dans le cloud.
Mais on ne peut pas se permettre de tous défendre de la même façon.
Dans la vraie vie ce n'est pas possible de tout défendre pour la migration vers le cloud, il est nécessaire de cartographier le cloud pour identifier tous les process.
Le BIA permet d'analyser les chemins critiques en rapport avec les BI les RSSI travaillent en collaboration.

Ce BIA permet de définir si ont gardé ce service en interne et pourquoi ?

Si ont choisi le cloud il faut décider :

- Quel modèle de cloud ?
- Modèle de déploiement ?
- Type de datacenter ?

RSSI inventaire des biens :

- Quoi protéger quel bien (tout ce qui appartient ou est contrôlé par l'entreprise),
- A quoi servent ces bien "uniquement économique" ?
- Ce que je dois protéger à quoi ça sert de le protéger ?
- Les inventaires automatisés ne suffissent pas c'est une partie d'eux

Inventaire :

- Voir les comptables (se mettre le comptable dans la poche),
- Logiciels inventaire,
- Rentrer dans les bureaux

La définition de bien :

- Matériels,
- Immatériel
- Process
- Chemin critique,
- Salariés

Dans le BIA il va falloir que l'on évalue la valeur de ses bien au sein de l'entreprise ce qui nous permet de définir le chemin critique. Mais comment on évalue les biens ?
Evaluer la valeur matérielle est facile mais évaluer le subjectif est plus complexe (humain et data…) Ce n'est pas au manager du service d'évaluer la valeur des données subjectives.
La valeur d'un processus et la somme des bien s su laquelle repose ce processus cela permet de déterminer le bon chemin critique.

Si le bien est critique il va avoir un impact majeur sur l'entreprise ne cas de défaillance.
L'expert cyber doit identifier tous les processus et doit réfléchir à l'entreprise et pas seulement à l'informatique.
L'expert cyber doit déterminer un SPOF (Single Point Of Failure) -> point de rupture des process un seul petit élément qui peut tout faire dérailler. Toute procédure est faillible.

Le SPOF est généralement dû au matériels ou un salarié (volontaire ou involontaire).

Ou l'humain peut mettre le bordel ou les équipements matériels peuvent mettre le bordel.

Avant le passage dans le cloud éliminer un maximum de SPOF !

Jun risque c'est la probabilité qu'un événement négatif interviennent, il faut que l'entreprise identifie tous les SPOF ce qui permet de rédiger la politique de gestion des risques au sein de l'entreprise.

Différentes politiques de gestion des risques :

- Evitement : trop compliquer à gérer pour moi je ne mets plus dans ce marché
  Ex covid machine à café -> risque trop élever on enlève les machines à café
  Je ne suis pas capable de le mitiger je n'opère plus dans ce secteur.
- Acceptation : on sait que le risque existe et je ne fais aucun effort pour mitiger ce risque
- Transfert du risque par exemple auprès d'une SSII
- Atténuation : mitiger l'impact de ce risque sur la productivité

Lors du passage au cloud on supprime certains risques (panne) en revanche on augmente le risque de cyber attaque et de data leak. On supprime le risque en créer mais on va en augmenter d'autres.

Si le data center s'il y a une attaque ça sera vous qui serez responsable :

-1 celle du directeur en premier
- 2 celle du RSSI

Il faut faire intervenir un juriste qui va lire les SPOF dans les contrats des hébergeurs. C'est toujours ou presque les hébergeurs qui rédige les contrats les hébergeurs décharge un maximum leur responsabilité. Dès que juridiquement c'est flou c'est un problème. C'est très très flou surtout hors France car la réglementation qui sera appliquer sera celle ou les data sont stockées.

On transfère la responsabilité technique mais on augmente la responsabilité juridique.
On ne peut pas transférer la responsabilité juridique. On est conscient des risques a passer dans le cloud.

Recommandation ANSSI :

- Le hardening des équipements fournisseurs, que le fournisseur cloud ferme les ports inutilisé, copte utilisateurs désactivés,
- Imposer les politiques de mots de passe sur les solutions SaaS et PaaS
- Interdiction d'avoir un compte d'administrateur globales, (le compte admin qui à le droit sur tout ça ne doit plus exister),
- Exiger les logs de modifications de configuration de nos serveurs,
- Vérifier que tous les services qui ne sont pas utile les désactiver,
- On ne laisse que ce dont a besoin
- Je veux savoir qui a accédé à mon serveur et quand et je veux avoir les preuves vidéo,

- Imposer un délai de mise à jour le délai des maj par apport au CVE,

Si ce n'est pas dans votre contrat c'est à votre désavantage, on réduit le risque

Négociations longues est compliquer

Mais le client à nécessité aussi de mettre en place des process :

- Pour les assurances
- Les PC qui accèdent au cloud doivent avoir un anti-malware les mises à jour de poste toujours réalisé,
- Possibilité de faire le check avec le DHCP et AAA,
- Les données de vos utilisateurs il faut chiffrer le disque dur sur tous les postes (mot de passe de démarrage du DD),
- Sauvegarde des données
- VPN sécuriser avec les bon algo RSA && AES
- Installer DLP (data lost prevention) (sauvegarde et la prévention du leak de data)
  Ce sont des dispositifs qui relevé les leak de données ca s'installe autant le cloud que dans le SI interne
- Les data doivent être chiffré dans votre poste dans le transport (SSH, HTTPS,)
  Dans le cloud DB ou DD soit chiffrer
  Et que l'accès à la ressource distante authentifie les utilisateurs qui souhaite accéder à la data

En moyenne une information au bout de 5 ans n'a plus aucune valeur (en général) dans les entreprises. Il faut déterminer au bout de combien de temps :

- On archive les data,
- On détruit les data,

Transiter dans le cloud nécessite de mettre en place une gestion du cycle de vie des données.

Les données doivent rester chiffre jusqu'à la phase de destructions !

L'objectif est de déchiffrer uniquement depuis le client final !

Les responsabilités :

Il y des responsabilités lorsque l'on gère des données sensibles.
Partage de risque, ça aboutie à une contractualisation des responsabilités de chacune des parties. Quoi que ce qu'on l'écrit dans ce contrat c'est l'entreprise qui fait appel au fournisseur cloud qui est responsable, car le client est propriétaire des données. Quand il y a une fuite de données c'est toujours l'entreprise qui est responsable du préjudice. Sauf si on le contractualise.

L'hébergeur est responsable sur la disponibilité des données, ils ne sont pas responsables des données.

Le client est propriétaire des données.

Il est possible de contractualiser des services :

- L'hébergeur s'engage à mettre le firmware à jour en moins de 24H,

Dès que l'on met quelque chose dans le cloud il faut définir les responsabilités. Il faut contractualiser, par exemple chez Jaguar Network il est possible de faire des contrat custom pour les responsabilités.

On est propriétaire des données donc responsable en cas de vol de données mais il faut définir avec le prestataire (fournisseur) les responsabilités.

En règle générale les fournisseurs vont tenter d'être le plus flou possible mais nous du coup on va essayer de prendre le plus de droits d'administration pour superviser la sécurité.

Le paradoxe : Le fournisseur lâchera le moins de lest et nous de notre coté on va prendre un maximum de données pour blinder le truc.

Cloud communautaire, plusieurs filiales d'un grand groupe qui construise leur cloud privé.
Cloud privé, cloud privé construit par une entreprise elle est propriétaire et propriétaire des données.

Si mon entreprise veut migrer dans le cloud : Il faut faire venir un migrateur cloud, qui soumet une feuille d'analyse de risque (coût, sécurité, avantage)

Les risques du cloud privé, c'est notre entreprise qui va gérer notre politique de sécurité du cloud privé, établir un PSSI et c'est la direction générale qui doit choisir (GPO, accès physique au bâtiment, politique de sécurité). Mais le problème c'est que c'est le cloud on ne connais pas la politique de sécurité.

Cloud privé == gestion du changement c'est beaucoup plus cher que d'aller chez jaguar, OVH. Mais on récupère la gestion des données, cela va marcher dans les grandes entreprises.

Menace :

- Non intentionnel,
- Mal intentionnel,
- Attaque interne,

- Attaque externe (facilitateur)
- Attaque externe dans le cloud privé si on a nos services chez OVH pas de problème leur SOC, CERT est rodé pour ça en cas d'attaque externe les équipe ne sont pas formé au moins que l'on soit une très grosse structure et qu'ils sont régulièrement entrainé, OVH sont très bon pour défendre leur infrastructure,

Dans le cloud privé il faut entrainer les équipes. La disponibilité va être garantie dans un cloud externe il bien plus efficace d'aller voir Orange Cyberdéfense que d'attendre que OVH nous défendent. La façon de gérer les données entre les pays du monde ne sont pas la même.

Cloud communautaire :

- **Les points d'entrées :** Le principal risque dans le cloud communautaire ce sont les points d'entrées, puisque c'est communautaire c'est gérer par plusieurs boites. Plus il y a d'entreprise sur ce cloud communautaire il ne suffit qu'une entreprise soit attaqué pour que toute l'autre entreprise soit impactée,
- **L'harmonisation :** toute l'entreprise applique les mêmes politique interprète, s'entendre sur les procédures et qu'elles les appliquent de même façon, Personne n'est là pour imposer des décisions ça va prendre du temps beaucoup de temps la coordination est très complexe,

Cloud public :

- Toutes les conditions si l'on veut faire des économies,
- Ça marche bien car ça permet donne l'impression que l'on se décharge des responsabilités,
- Une partie du cloud communautaire peux arriver,
- Verrouillage dans la technologie propriétaire du constructeur,
- La récupération de données coute très cher, facturé à la volumétrie, il faut vérifier tout ça,
- On a le sentiment que tout est infinie mais ce fournisseur cloud (on connais la marque des serveurs que l'on utilise, le fournisseur qui fournis les serveurs au fournisseur cloud si c'est un fournisseur russe ça pose peut-être des problèmes)
- Se méfier des offres trop attractives,
- Problème juridique de l'endroit où se trouve les données,
- Conflit d'intérêt je suis l'administrateur qui s'occupe de Véolia et l'autre de Suez environnement,

Cloud privé :

- Tous les risques du cloud public existent dans le cloud privé,

IAAS :
On vous fournit serveur + réseau et après vous vous débrouiller

- Erreur humaine, le personnel du cloud est responsable de la maintenance physique du serveur, on peut nous voler le disque dur mais normalement on peut chiffrer le disque dur permet de prévenir le vol de données,
- Menace des failles CVE, applicatif…
- En interne on ne sait pas c'est bien fait en générale dans el cloud on sais que c'est bien fait

PAAS :
Le fournisseur cloud fournis l'OS, c'est lui qui durcit l'OS.

- **Incompatibilité** entre l'OS durcit et l'application de l'entreprise,
- Il y a des failles dans les hyperviseurs (promiscuité, les failles 0day) il y a des failles on peut récupérer des données dans des VM verrouiller de la VM vers hyperviseur soit hyperviseur VM soit VM -> VM,
- Image de l'OS corrompue

Type d'hyperviseur

- T1 (Esxi, Xen, Hyper-V car il démarre avant l'OS) plus dur à compromettre
- T2 (Workstation, Virtual Box..)

Faire transiter des données entre deux VM faille de **bleeding** :

- **Gest escape**, un utilisateur dans une VM il arrive à s'échapper du confinement de cet VM mauvaise config, fail, le il va arriver sur l'hyperviseur et obtenir des données d'une autre VM,
- **Host escape**, l'attaquant à réussi à obtenir des informations d'une autre VM et à en prendre le contrôle,

ESXI avec toutes les options la mémoire qui est attribué entre les VM est remise à 0 mais ca coute cher.

SAAS :
Software, les applicatif ne sont pas mis à jour

- Les patchs ne sont pas déployés,

Fournisseur :

- Sécurité physique :
  - Hardening serveur (bios, chiffrement physique, maj firmware, hyperviseur VM, gestion centralisée, communication LAN chiffrés (serveur -> SAN), Démarrage impossible GRUB mon utilisateur)
  - Accès physique,

- Exiger à son fournisseur de travailler avec des **Template**, modèles sécurisés pour un type d'équipement -> connaissance des règles de sécurités implémentée,

- Monitoring, le fournisseur collecte suffisamment de log pour qualifier et investiguer les incidents,

- Configuration des accès distant (si on en IaaS et que l'on a un routeur virtuel Cisco on ne va pas se déplacer pour configurer le routeur chez le fournisseur c'est la responsabilité du fournisseur de faire une configuration minimale pour que l'on puisse administrer le routeur pareil pour les serveurs et de préférence en SSH, HTTPS) c'est de la responsabilité du fournisseur de **maintenir** et de **sécuriser** ces accès distants si c'est du SaaS le fournisseur s'engage à créer un compte pour administrer l'application il faut que ca soit écrit dans le contrat,

- Pare feu : ça reste de la responsabilité du fournisseur de le configurer,

- IDS/IPS : si l'on met nos données dans le cloud il faut que le fournisseur nous garantisse une surveillance active ou passive des flux applicatifs si ce genre de mécanisme le client est en droit une copie des logs vous concernant

- Honeypot : présence + monitoring c'est un serveur vulnérable qui à l'ai un peu plus facile a attaquer que notre serveur l'honeypot est couplé à l'IPS pour voir combien ils sont et leur technique

- Vulnerability Assement : Le data center est très clair sur sa politique de vulnerability assement soit on négocie avec lui de réaliser du vulnerability assement,

SSO
IAM : *Identifiy Access Management*

- **Gestion des identités**,
  - Dépôts des identités (information attributs personne, compatible avec AD, x500, LDAP, il existe des templates les droits ne sont pas écrits dedans mais cela permet de structurer les droits)
- **Gestion des droits**, (applications multiples, règles d'accès liste des objets et le profil nécessaire pour y accéder)
- **Fédération des** identités elle va proposer du SSO entre plusieurs entreprises, (OAuth HTTPS fournir un mot de passe généralement sur les téléphones et l'autre OpenId qui est un fork de Oauth V2 pas beson de mot de passe),

C'est ce qu'on appelle adminstrer en SILO

Si je vole la BDD de l'un je ne peux pas tout exploiter.
Le lien entre les deux c'est ce que l'on appelle le SSO.

On va associer que l'on va lier
J'ai un jeton avec mon profil d'identité et c'est l'application va tester le jeton si j'ai le droit d'y accéder.

Le contrôleur m'authentifie et l'application vérifie si j'ai les droits d'accéder à l'application.

Mise ne place d'un **WAF** c'est un pare feu applicatif, il connait le fonctionnement normal de l'application qu'il protège un WAF == une application ça fait de la deep inspection il déchiffre le trafic. La règle c'est un 1 WAF une application. Le WAF connais la façon normale d'une application dès que ça diverge d'une utilisation normale.

Le **DAM**, Database Activity Monitoring, son objectif est de surveiller des activités anormales de la base de données (bloquer des transactions, bloquer des select) C'est un plugin qui vient sur le serveur de base de données.

Il existe deux types d'API :

- REST (REpresentational State Transfert), échanger des données entre des URL, XML, JSON
- SOAP (Simple Object Access Protocol) échange entre deux applications favoriser sur les échanges web a favoriser entre échange web on peux mettre du SOAP dans du SMTP, http, FTP est généralement c'est structuré en XML
    - On préconise le SOAP pour les échanges entre application car :
        - Gestion des erreurs avancée,
        - Très strict dans le format des échanges

Une fois que tout le process est réalisé il faut passer tout ces process dans la moulinette de l'OWASP