

SECURITE DANS LE CLOUD

Master 1 Sécurité et Administration Système

Dr GOUHO BI JEAN BAPTISTE
CONSULTANT-FORMATEUR EN CYBERSECURITE

Introduction

Ce support de cours a pour but de donner dans un premier temps les bases des systèmes de virtualisations utilisés en entreprise, ensuite présenter la notion de cloud computing et parler des menaces liées au cloud et les contremesures pour lutter contre ces menaces.

Cette virtualisation en termes de machines virtuelles utilisées pourra être mise en œuvre dans une plate-forme hébergé en ligne de type cloud.

Ce cours sera divisé en 3 parties :

- La partie 1 traitera des concepts de bases de la virtualisation ;
- La partie 2 parlera du cloud computing ;
- La partie 3 traitera des menaces liées à la virtualisation et au cloud computing.

VIRTUALISATION

La virtualisation fait référence à l'abstraction physique des ressources informatiques. Cela veut dire que les ressources physiques allouées à une machine virtuelle sont abstraites à partir de leurs équivalents physiques. Les disques virtuels, les commutateurs virtuels, les interfaces virtuels, les processeurs virtuels correspondent à des ressources physiques sur les systèmes informatiques.

La virtualisation a des multiples avantages comme :

- Une meilleure gestion du temps de restauration des machines, car avec les machines physiques ce temps pouvait être long en cas d'incident ;
- Permettre de lutter contre le vieillissement de l'infrastructure physique ;
- Minimiser les coûts matériels ;
- Equilibrer les charges ;
- Tester des logiciels ;
- Déployer des serveurs plus rapidement ;
- Economiser de l'énergie ;
- Sécurisation et gestion des risques.

1. Terminologie et concepts

- Para-virtualisation

Technologie de virtualisation logicielle basée sur l'utilisation d'un hyperviseur et optimisée pour ce type de fonctionnement.

- Hyperviseur

Système basé sur l'utilisation d'un noyau hôte allégé et optimisé, utilisé pour faire fonctionner simultanément plusieurs systèmes d'exploitation sur une même plate-forme matérielle.

- Virtualisation matérielle

Technologie de virtualisation basée sur l'utilisation de ressources de type matérielles. Intel (Intel VT) et AMD (AMD-V) proposent une gamme de processeurs dédiés à la virtualisation matérielle.

- Virtualisation du système d'exploitation

Technologie de virtualisation dont le principe est l'exécution d'un système d'exploitation dans un contexte isolé des ressources matérielles de la plate-forme hôte.

- Virtualisation d'applications

Technologie de virtualisation dont le principe est la mise à disposition et l'exécution d'une application dans un contexte isolé des ressources du système d'exploitation de la plate-forme hôte.

- Machine virtuelle

Environnement émulé et isolé, utilisé pour supporter le contexte d'exécution d'un système d'exploitation ou d'un programme sur une machine hôte. Le terme invité est quelque fois utilisé pour désigner une machine virtuelle.

- **Hôte**

Machine physique destinée à héberger les environnements virtuels.

- **Hub applicatif**

Référentiel central pour la mise à disposition et la distribution de ressources distantes et virtualisées.

- **Emulation**

Action de reproduction du contexte d'exécution d'un système sur un autre.

- **Isolation**

Environnement d'exécution cloisonné sans interférence avec les ressources installées localement.

On peut identifier pour les solutions de virtualisation deux domaines d'application :

- La virtualisation de plates-formes/systèmes d'exploitation ;
- La virtualisation de ressources et contenus.

Chacun de ces domaines propose un panel de technologies et de solutions offrant de nombreuses fonctionnalités pour répondre aux principaux besoins informatiques.

2. Virtualisation des serveurs

La solution de virtualisation de serveurs consiste à partager les ressources d'une plate-forme matérielle appelée hôte vers plusieurs systèmes invités dénommés machines virtuelles.

Le schéma de la figure 1 illustre le principe de l'architecture de la virtualisation de serveurs.

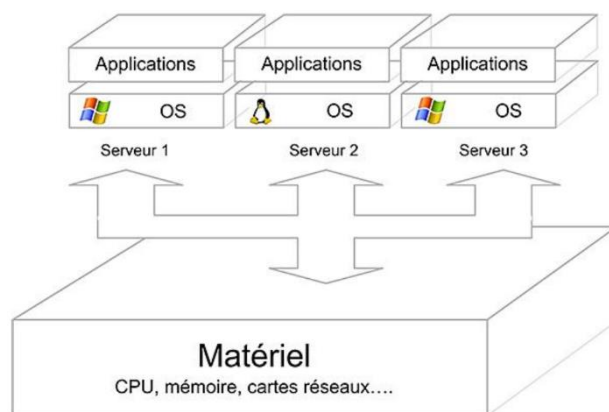


Figure 1

3. Virtualisation d'applications

L'objectif de la mise en œuvre d'une solution de virtualisation d'applications est d'assurer le fonctionnement des applications dans un contexte d'exécution indépendant et isolé du système d'exploitation client. Le contexte d'exécution ainsi isolé, sécurise le fonctionnement de l'application avec la plate-forme d'exécution.

La figure 2 illustre le principe de fonctionnement d'une application virtualisée dans un environnement d'exécution isolé.

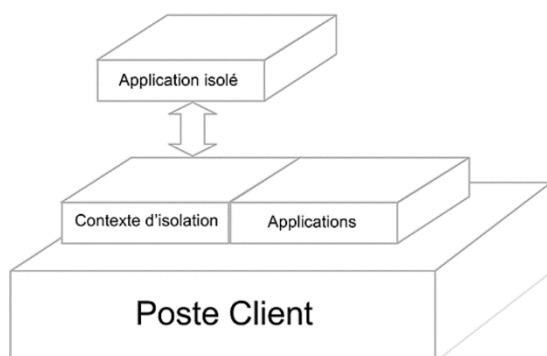


Figure 2

4. Virtualisation de poste de travail

La virtualisation de poste de travail communément appelée VDI (Virtual Desktop Infrastructure), offre à un utilisateur à partir d'une machine virtuelle, un environnement de bureau complet, comprenant le système d'exploitation et les applications.

Le schéma de la figure 3 illustre le principe de l'architecture de la virtualisation de poste de travail.

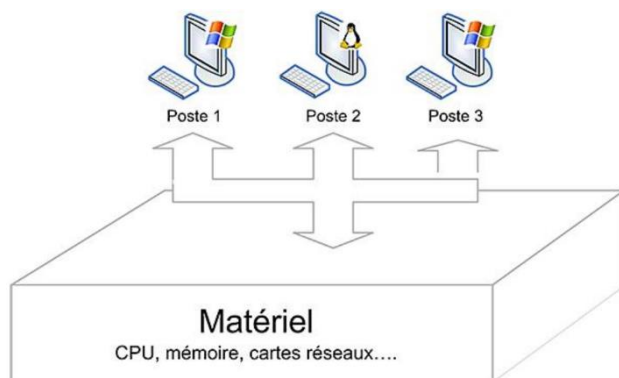


Figure 3

5. Sécurisation des environnements virtualisés

Le premier aspect de la sécurisation des environnements virtualisés est le cloisonnement des environnements d'exécution d'applications afin d'éviter la corruption de données inter environnements. Les données doivent être segmentées et organisées suivant leur niveau de criticité et de sensibilité.

Le schéma de la figure 4 illustre le principe de consolidation et de segmentation par zones de sécurité de ressources de type de serveurs.

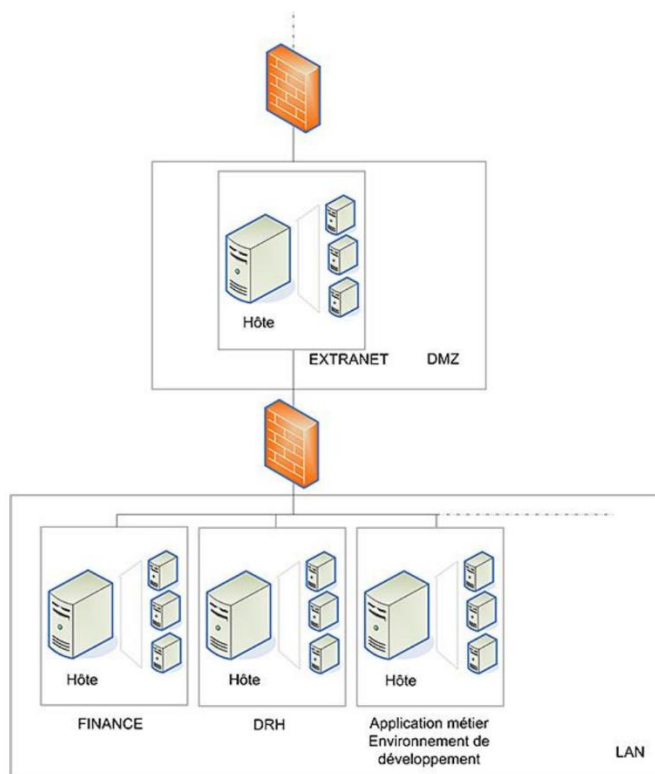


Figure 4

Dans ce exemple, les données de la plate-forme de la DRH ne sont pas visibles à partir de l'hôte ou d'une des machines virtuelles de la plate-forme du service financier de l'entreprise. Une indisponibilité de la plate-forme de développement des applications métier n'impacte pas la disponibilité des autres plates-formes. Cette organisation permet de bien gérer les sessions de maintenance des plates-formes virtualisées.

6. Solutions de virtualisation

Trois constructeurs dominent le marché des technologies de virtualisation. Ce sont :

- VMWare avec sa solution VMWare ESX ;
- Microsoft avec sa solution Hyper V ;
- Citrix avec sa solution Citrix Xen.
- Au niveau des solutions libres de la famille des KVM (Kernel Virtual Machine), nous avons Proxmox qui est une solution utilisée en entreprise pour la virtualisation de serveurs.

CLOUD

Le monde de l'informatique a beaucoup évolué depuis l'apparition des PDA (Personal Digital Assistant) qui sont devenus aujourd'hui des « smart phones ».

Traditionnellement l'on avait un utilisateur avec son ordinateur ayant un accès à internet pour des recherches. Cela est illustré sur la figure 1.

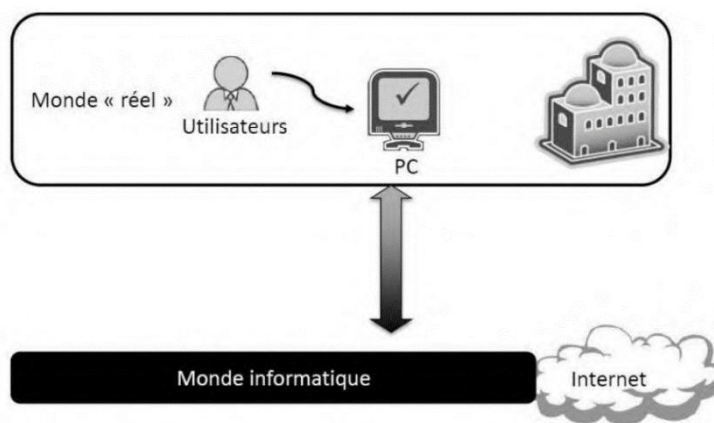


Figure 1

Aujourd'hui l'écosystème informatique est devenu un environnement collaboratif où évolue plusieurs technologies différentes. Le « cloud computing » où informatique dans les nuages permet de faire la synthèse de toutes ces technologies que doivent utiliser les utilisateurs pour travailler. La figure 2 illustre cette évolution.

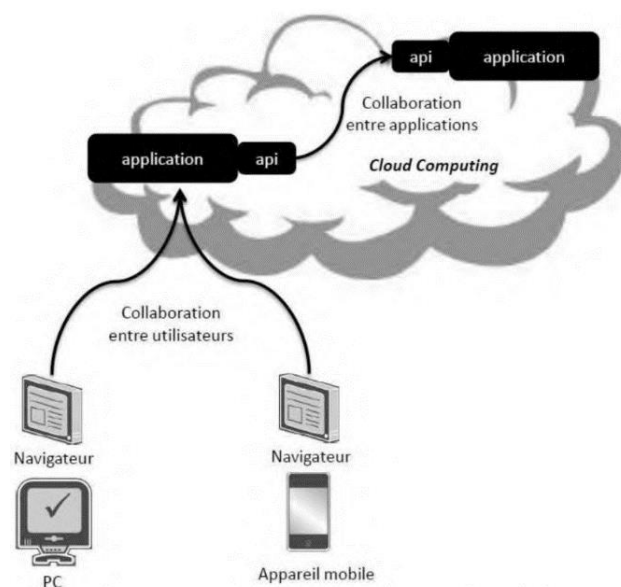


Figure 2

Le cloud computing peut donc être vu comme l'utilisation d'une plateforme informatique à l'échelle d'internet. Cela permet d'avoir accès à des machines situées partout dans le monde sur lesquelles peuvent tourner des services différents. La figure 3 illustre bien cette évolution de l'informatique grâce au cloud.

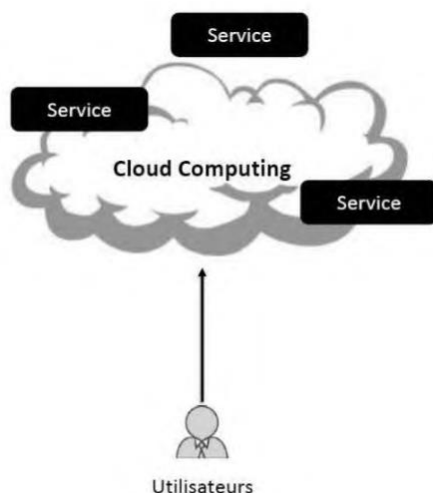


Figure 3

Le cloud est une évolution des technologies de virtualisation comme :

- La mutualisation des ressources ;
- Abstraction sur la localisation ;
- Elasticité.

Le cloud reprend ces propriétés de la virtualisation mais à plus grande échelle mais ajoute d'autres propriétés à celle de la virtualisation comme :

- Le Pay As You Go : dans ce concept, les utilisateurs paient les ressources qu'ils utilisent en fonction de leur consommation réelle et précise. Ce qui permet au responsable informatique de savoir informatique d'une personne ou de telle application.
- Le Self-Service : l'équipe de développement peut demander l'allocation de ressources via un portail web et l'avoir quelques minutes plupart.
- Les API ouvertes : le cloud propose des API (Application Programming Interface) accessibles à distance cela permet donc de les intégrer avec le système d'information et aussi de piloter des services à distance.

Cela permet de donner une définition assez simple du cloud computing comme :

Cloud computing = virtualisation + Pay As You Go + Self-service + API ouvertes

Cela est illustré sur la figure 4.

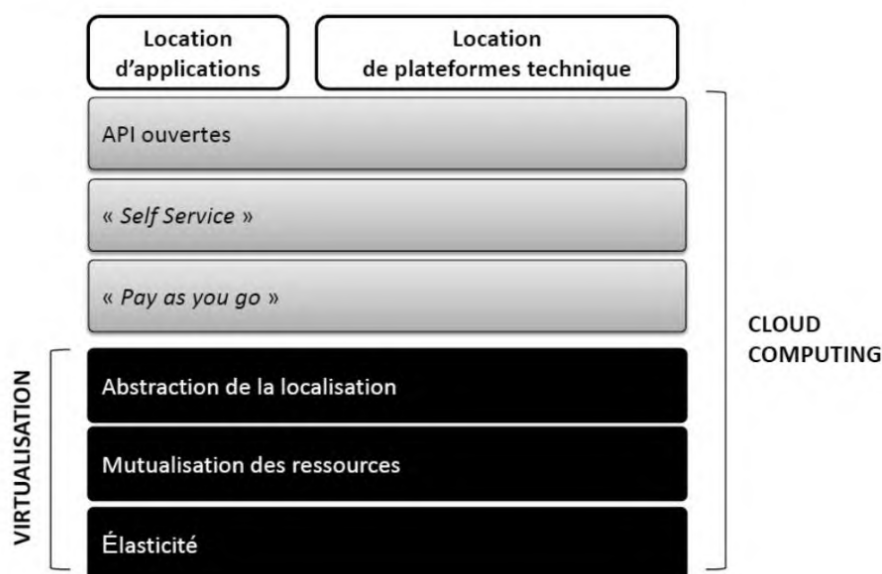


Figure 4

Le concept de cloud computing englobe les concepts SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service).

1. SaaS

Le concept de SaaS est un logiciel fourni comme un service c'est-à-dire la location d'une application opérationnelle.

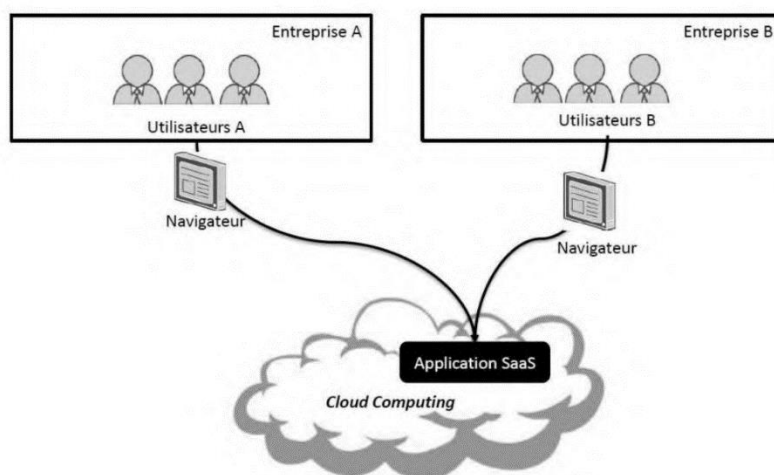


Figure 5

Avantages

Pas de dépenses d'investissement. Les utilisateurs n'ont pas de coûts initiaux.

Agilité. Les utilisateurs peuvent fournir à leurs employés un accès aux dernières versions des logiciels rapidement et facilement.

Modèle tarifaire de type paiement à l'utilisation. Les utilisateurs paient pour le logiciel qu'ils utilisent selon un modèle d'abonnement, généralement mensuel ou annuel, quelle que soit leur utilisation du logiciel.

Compétences. Aucune compétence technique approfondie n'est nécessaire pour déployer, utiliser et tirer parti des avantages du modèle SaaS.

Flexibilité. Les utilisateurs peuvent accéder aux mêmes données d'application où qu'ils se trouvent.

Inconvénient

Limitations des logiciels. Il peut y avoir certaines limitations à une application logicielle, qui peuvent affecter la façon dont les utilisateurs travaillent. Comme vous utilisez le logiciel tel quel, vous n'avez pas de contrôle direct sur les fonctionnalités. Quand vous évaluez la plateforme SaaS la mieux adaptée à une charge de travail, veillez à prendre en compte l'ensemble des besoins métier et des limitations des logiciels.

2. PaaS

PaaS désigne la location d'une plate-forme technique pour l'exécution de code développé donc désigne une plate-forme d'exécution hébergée par un opérateur et accédée depuis internet.

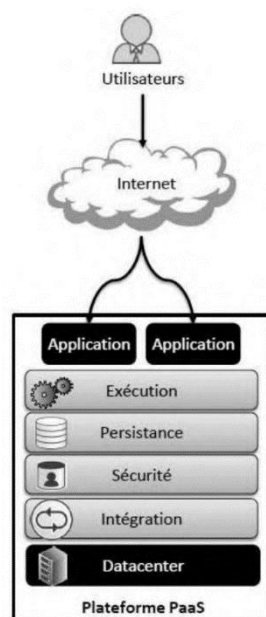


Figure 6

Avantages

Pas de dépenses d'investissement. Les utilisateurs n'ont pas de coûts initiaux.

Agilité. PaaS est plus agile que IaaS, et les utilisateurs n'ont pas besoin de configurer des serveurs pour exécuter des applications.

Modèle basé sur la consommation. Les utilisateurs paient seulement pour ce qu'ils utilisent et fonctionnent selon un modèle de dépenses de fonctionnement.

Compétences. Aucune compétence technique approfondie n'est nécessaire pour déployer, utiliser et tirer parti des avantages du modèle PaaS.

Avantages du cloud. Les utilisateurs peuvent bénéficier des compétences et de l'expertise du fournisseur de cloud pour garantir que leurs charges de travail sont sécurisées et hautement disponibles. Ils peuvent aussi accéder à davantage d'outils de développement de pointe. Ils peuvent ensuite appliquer ces outils tout au long du cycle de vie d'une application.

Productivité. Les utilisateurs peuvent se concentrer uniquement sur le développement d'applications, car fournisseur de cloud réalise l'ensemble de la gestion de la plateforme. Il est plus facile de travailler avec des équipes distribuées en tant que services, car l'accès à la plateforme s'effectue via Internet. Vous pouvez rendre la plateforme disponible dans le monde entier plus facilement.

Inconvénient

Limitations des plateformes. Il peut y avoir certaines limitations à une plateforme cloud, qui peuvent affecter la façon dont une application s'exécute. Quand vous évaluez la plateforme PaaS la mieux adaptée à une charge de travail, veillez à prendre en compte toutes les limitations dans ce domaine.

3. IaaS

Il s'agit de location de plateforme technique permettant l'exécution d'architectures applicatives complètes comprenant base de données, serveurs d'applications etc.

Les IaaS s'adressent aux équipes d'exploitations comme les ingénieurs systèmes et réseaux.

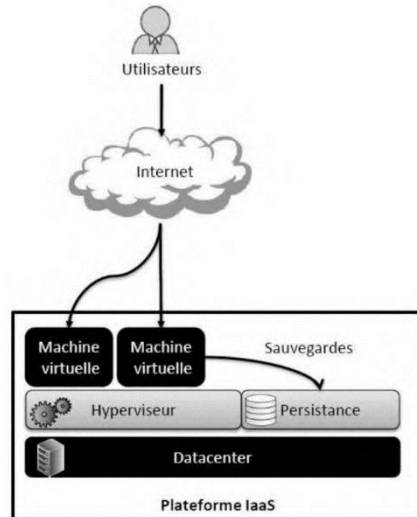


Figure 7

Avantages

Pas de dépenses d'investissement. Les utilisateurs n'ont pas de coûts initiaux.

Agilité. Les applications peuvent être rendues accessibles rapidement, et dé provisionnées chaque fois que c'est nécessaire.

Gestion : Le modèle de responsabilité partagée s'applique : l'utilisateur gère et maintient les services qu'il a provisionnés, et le fournisseur de cloud gère et maintient l'infrastructure cloud.

Modèle basé sur la consommation. Les organisations paient seulement pour ce qu'elles utilisent et fonctionnent selon un modèle de dépenses de fonctionnement (OpEx).

Compétences. Aucune compétence technique approfondie n'est nécessaire pour déployer, utiliser et tirer parti des avantages d'un cloud public. Les organisations peuvent utiliser des compétences et de l'expertise du fournisseur de cloud pour garantir que les charges de travail sont sécurisées et hautement disponibles.

Avantages du cloud. Les organisations peuvent utiliser des compétences et de l'expertise du fournisseur de cloud pour garantir que les charges de travail sont sécurisées et hautement disponibles.

Flexibilité. IaaS est le service cloud le plus flexible, car vous avez le contrôle de la configuration et de la gestion du matériel exécutant votre application.

On peut résumer une plate-forme cloud avec le tableau 1.

Tableau 1

Plateforme	Interne	IaaS	PaaS	SaaS
Applications	-	-	-	☑
Environnement exécution	-	-	☑	☑
Base de données	-	-	☑	☑
Système d'exploitation	-	-	☑	☑
Hyperviseur	-	☑	☑	☑
Machines	-	☑	☑	☑
Réseaux	-	☑	☑	☑

D'un point de vue utilisateurs finaux du cloud cela peut être résumé comme suit :

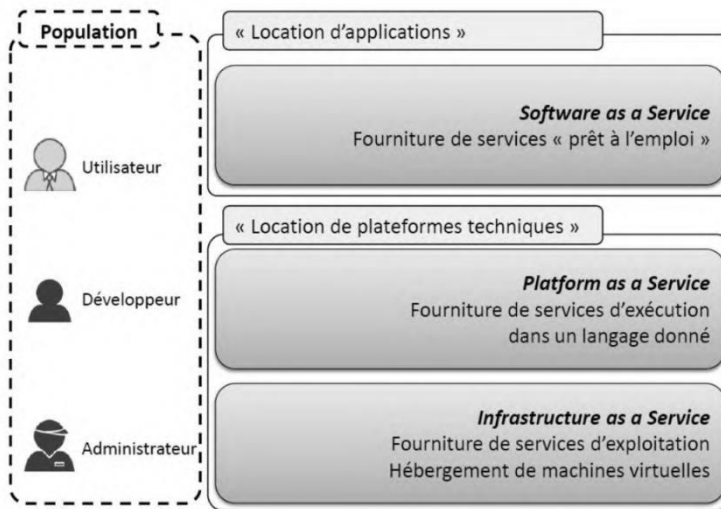


Figure 8

Le graphique suivant illustre les différents niveaux de responsabilité entre un fournisseur de cloud et un locataire de cloud.

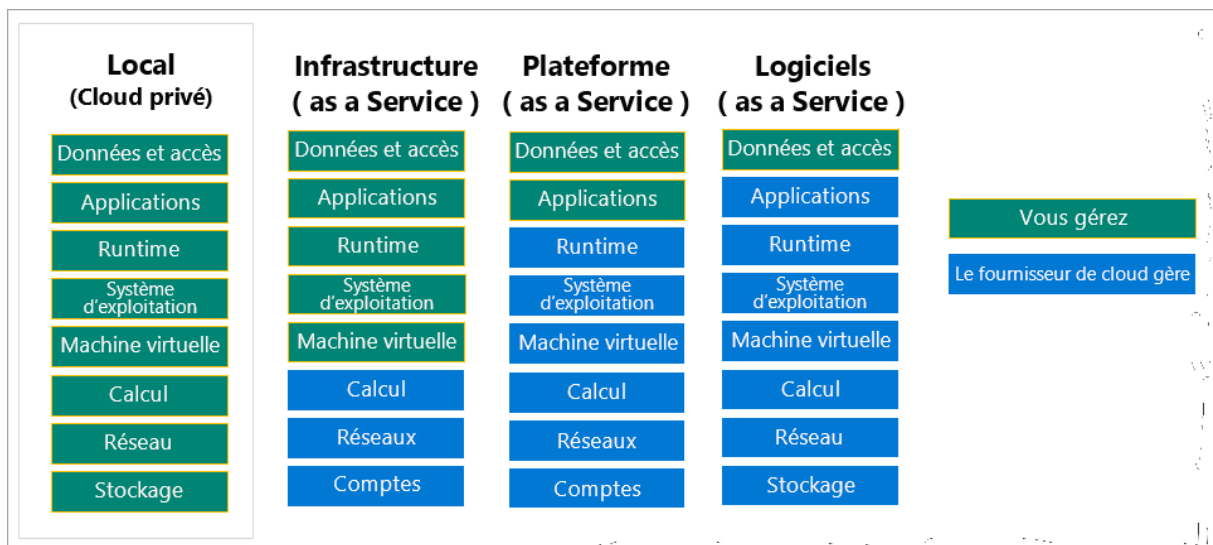


Figure 9

4. Modèles de déploiement

Il existe 4 modèles de déploiement.

a. Cloud privé

L'infrastructure cloud est utilisée par une seule organisation. Elle peut être gérée par l'organisation ou par une tierce partie. L'infrastructure peut être placée dans les locaux de l'organisation ou à l'extérieur.

b. Cloud communautaire

L'infrastructure cloud est partagée par plusieurs organisations pour les besoins d'une communauté qui souhaite mettre en commun des moyens (sécurité, conformité, etc.). Elle peut être gérée par les organisations ou par une tierce partie et peut être placée dans les locaux comme à l'extérieur.

c. Cloud public

L'infrastructure cloud est ouverte au public ou à de grands groupes industriels. Cette infrastructure est possédée par une organisation qui vend des services cloud.

d. Cloud hybride

L'infrastructure cloud est composée d'un ou plusieurs modèles cités plus haut mais qui restent des entités séparées. Ces infrastructures sont liées entre elles par la même technologie qui autorise la portabilité des applications et des données.

5. Comparaison entre les modèles cloud

a. Cloud public

- Aucune dépense en capital pour effectuer un scale-up.
- Les applications peuvent être rapidement configurées et dé provisionnés.
- Les organisations paient uniquement pour ce qu'ils utilisent.

b. Cloud privé

- Le matériel doit être acheté pour le démarrage et la maintenance.
- Les organisations disposent d'un contrôle total sur les ressources et la sécurité.
- Les organisations sont responsables de la maintenance et des mises à jour du matériel.

c. Cloud hybride

- Offre la plus grande flexibilité.
- Les organisations déterminent où exécuter leurs applications.
- Les organisations contrôlent la sécurité, la conformité ou les exigences légales.

Selon le type de déploiement, le cloud permet une optimisation de la gestion des ressources de l'infrastructure.

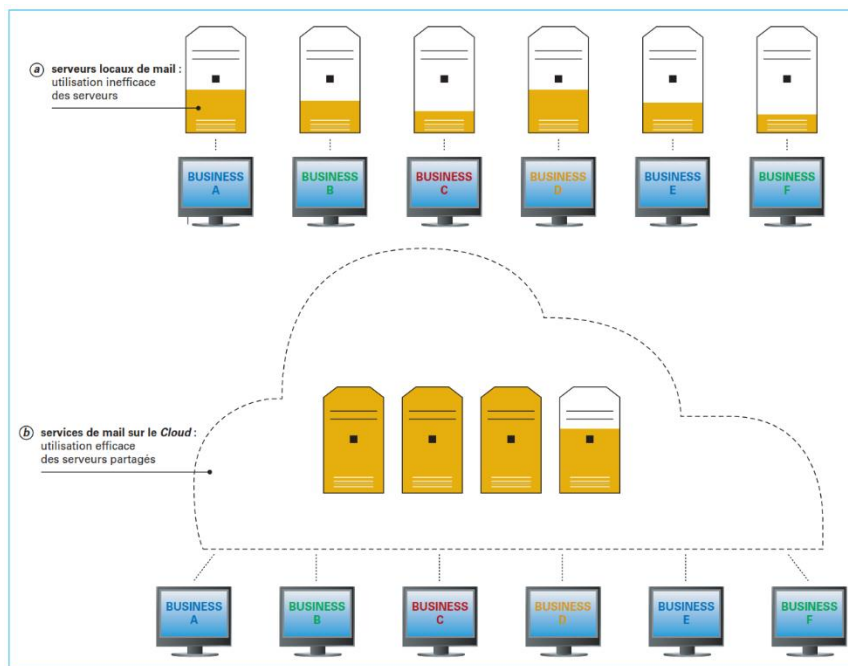


Figure 10

6. Dépenses d'investissement et frais d'exploitation

Deux types de dépenses sont à prendre en compte :

- Les **dépenses d'investissement (CapEx, Capital Expenditure)** sont les dépenses initiales consacrées à l'infrastructure physique, amortissables au fil du temps. Le coût initial des dépenses d'investissement a une valeur qui diminue au fil du temps.
- Les **dépenses de fonctionnement (OpEx, Operational Expenditure)** représentent les dépenses courantes liées aux services ou aux produits, facturées au fil de leur achat. Vous pouvez déduire ces dépenses au titre de l'année où vous les avez engagées. Il n'y a pas de coût initial, car vous payez pour un service ou un produit quand vous l'utilisez.

7. Solutions de cloud




Les principales solutions de cloud pour entreprise sont :

- Amazon Web Services (AWS)
- Microsoft Azure
- Google cloud
- Alibaba cloud
- Oracle cloud




Nous allons faire une comparaison des 3 solutions leaders dans le domaine du cloud que sont :

- Amazon Web Services (AWS)
- Microsoft Azure
- Google cloud

7.1 Présence

 <p>Amazon Web Services a 69 « availability zones » dans 22 locations géographiques. Amazon compte avoir 12 de plus dans un future proche.</p>	 <p>Microsoft Azure a 54 régions dans le monde et est disponible dans 140 pays.</p>	 <p>Google Cloud Platform est disponible dans plus de 200 pays dans le monde.</p>
---	---	--




7.2 Serveurs virtuels

 <p>AWS EC2 est un service web qui aide au redimensionnement de la capacité de calcul. Vous pouvez l'utiliser pour exécuter vos programmes sur une machine virtuelle.</p>	 <p>Azure Virtual Machine donne à l'utilisateur l'habilité de déployer et gérer un environnement virtuel dans un réseau virtuel dans le cloud.</p>	 <p>GCP VM instances permet à l'utilisateur de déployer et gérer des machines virtuelles dans le but d'y assigner une charge de travail dans le cloud.</p>
--	--	---



7.3 PaaS

 <p>AWS Elastic Beanstalk est un service d'orchestration qui aide au déploiement d'applications et aide à la maintenance de celles-ci.</p>	 <p>Azure Cloud Services permet d'utiliser une plateforme pour l'écriture de codes pour des applications sans avoir de soucis en termes de ressources matérielles.</p>	 <p>Google App Engine est un service utilisé par les développeurs pour développer et héberger des applications sur les data centers de google.</p>
---	--	---

7.4 Exécution sans serveur

 <p>AWS Lambda est un service utilisé pour exécuter du code « backend » il s'auto ajuste lors des exécutions lorsque cela est nécessaire.</p>	 <p>Azure Functions permet aux utilisateurs de créer des applications en utilisant de simples fonctions avec le langage de programmation de leur choix.</p>	 <p>GCP Cloud Functions permet d'exécuter votre code dans le cloud avec de la haute disponibilité et à la tolérance aux pannes.</p>
--	--	--

7.5 Stockage

 <p>Amazon S3 permet le stockage et la récupération d'objets dans le cloud.</p>	 <p>Blob Storage permet le stockage de données dans des niveaux, ces niveaux dépendent de comment l'on accédera à ces dit données.</p>	 <p>Google Cloud Storage permet un stockage unifié pour les données en live et ceux qui sont archivées.</p>
---	--	---

8. Concepts avancés du cloud

8.1 Conteneur (container)

Les conteneurs sont des unités de logiciel abstraites qui ont tout ce dont vous avez besoin pour gérer une charge de travail ou un processus. L'orchestration de conteneurs est la capacité à déployer et gérer plusieurs conteneurs dans l'infrastructure de Cloud privé et public.

Un conteneur est une enveloppe virtuelle qui permet de packager une application avec tous les éléments dont elle a besoin pour fonctionner : fichiers source, runtime, bibliothèques, outils et fichiers. Ils sont packagés en un ensemble cohérent et prêt à être déployé sur un serveur et son système d'exploitation.

Exemple : Amazon Elastic Container Service (ECS), Microsoft Azure Container Instances (ACI)

8.2 Docker

Docker est un logiciel libre permettant de gérer des conteneurs. Un conteneur est une abstraction qui regroupe le code et toutes ses dépendances afin que l'application s'exécute rapidement et de manière fiable d'un environnement informatique à un autre.

8.3 Kubernetes

Kubernetes est une plate-forme open-source extensible et portable pour la gestion de charges de travail (workloads) et de services conteneurisés. Elle favorise à la fois l'écriture de configuration déclarative (declarative configuration) et l'automatisation. C'est un large écosystème en rapide expansion.

Docker est une plateforme de conteneurisation et d'exécution, tandis que Kubernetes est une plateforme permettant d'exécuter et de gérer des conteneurs à partir de nombreux systèmes d'exécution de conteneurs. Kubernetes prend en charge de nombreux environnements d'exécution de conteneurs, y compris Docker.

Exemple : Amazon Elastic Kubernetes Service (EKS), Docker Kubernetes Service (DKS)

8.4 Microservices

Les microservices constituent une approche architecturale et organisationnelle du développement logiciel, dans laquelle le logiciel se compose de petits services indépendants qui communiquent via des API bien définies. Ces services sont détenus par de petites équipes auto-tenues.

Les microservices stimulent vos équipes et vos routines grâce à un développement distribué. Vous pouvez aussi développer plusieurs microservices simultanément. Ainsi, davantage de développeurs peuvent travailler en même temps, sur la même application, ce qui réduit la durée du développement.

Architecture. L'architecture microservices est basée sur des services plus petits et à plus fine granularité axés sur un seul objectif et pouvant fonctionner indépendamment les uns des autres, mais qui interagissent pour prendre en charge la même application.

SECURITE

1. Sécurité liée au concept de la virtualisation

Les problèmes de sécurité liés à la virtualisation peuvent avoir plusieurs origines. Selon un rapport de IBM X-Force de mars 2011 cela se repartit en 7 classes. Cela est illustré sur la figure 1.

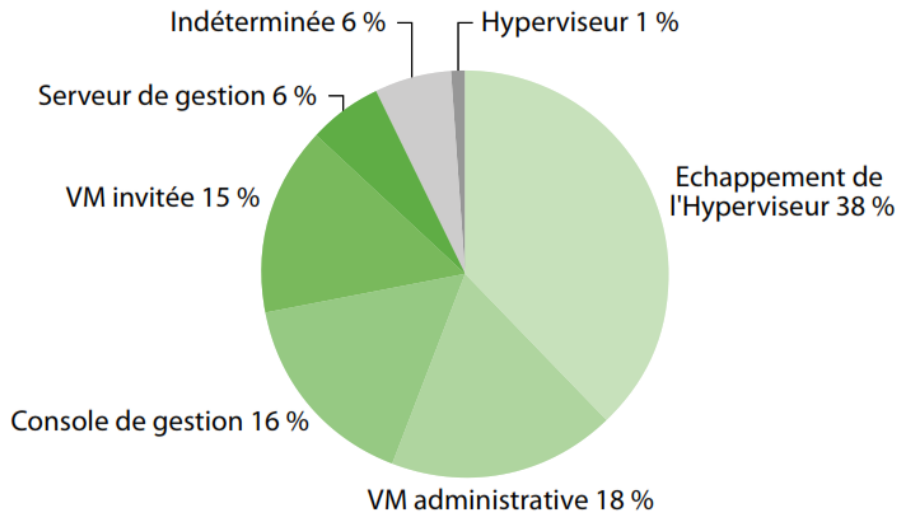


Figure 1

L'une des solutions est de renforcer la visibilité et la sécurité par l'utilisation d'une passerelle de sécurité virtuelle proposée par plusieurs sociétés comme : Fortinet, Check Point, Palo Alto, Cisco etc.

Dans cette approche connue sur le nom « end point security » une « appliance » virtuelle protège toutes les machines virtuelles.

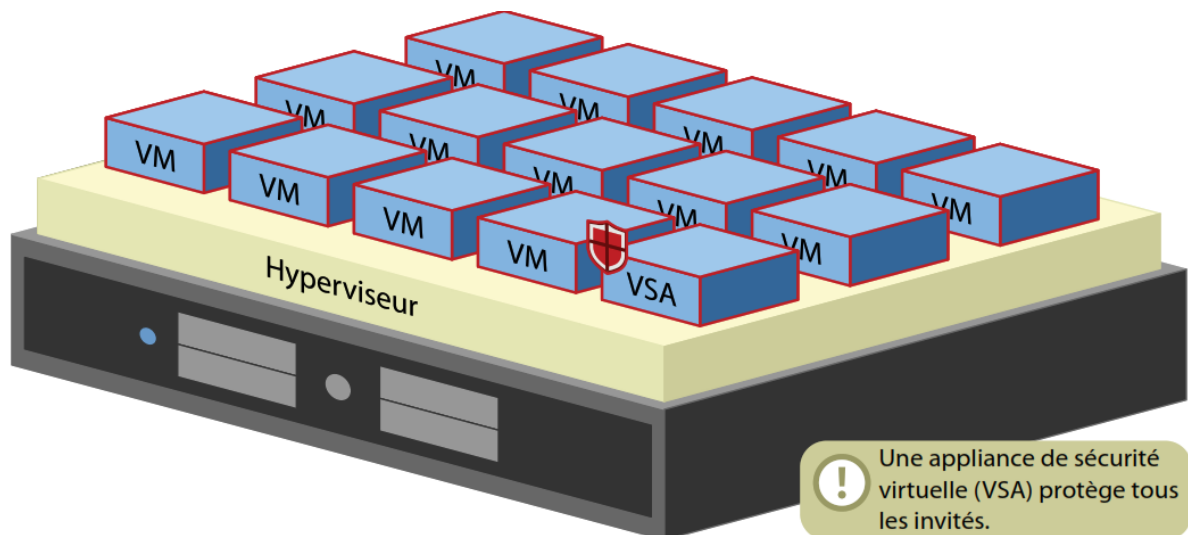


Figure 2

Pour améliorer la sécurité, il faut appliquer une politique « zero trust » cela implique une politique de gestion des accès et des identités (IAM).

L'une des voies de l'application de la politique « zero trust » est le cloisonnement au niveau des hôtes virtuels car cela permet de limiter la propagation d'un logiciel malveillant par une bonne segmentation et la limitation des communications entre machines virtuelles.

Cela est par exemple sur hyper V avec le gestionnaire de commutateur virtuel.

L'hyperviseur de Microsoft Hyper V permet de créer 3 commutateurs Virtuels :

- Externe : avec ce type de commutateur virtuel, il est possible d'utiliser la carte réseau de la machine hôte dans la machine virtuelle. Ainsi la machine virtuelle obtiendra une connexion sur le réseau physique pour lui permettre d'accéder à des ressources sur le réseau physique.
- Interne : cette option permet la création d'un réseau seulement entre la machine physique et les machines virtuelles donc il sera impossible aux machines virtuelles d'accéder au réseau local.
- Privé : la communication est seulement entre les machines virtuelles donc la machine hôte ne peut pas communiquer avec les machines virtuelles.

2. Sécurité liée au concept du cloud

La sécurité dans le cloud est une préoccupation majeure des entreprises. Les questions que l'on est amené à se poser est :

- Quelle confiance peut-on avoir dans le stockage des données à l'extérieur de l'entreprise ?
- Quels sont les risques associés à l'utilisation des services partagés ?
- Comment démontrer la conformité des systèmes à des normes d'exploitation ?

Les défis liés à la sécurité du cloud sont nombreux car il faut donner confiance dans le modèle de sécurité et dans les outils de gestion qui sont proposés.

2.1 composants de sécurité d'un système de cloud

Les différents composants qui participent à la sécurité d'un système cloud :

a. Service de console de gestion (provisioning)

Il est possible de mettre en service plusieurs instances dans plusieurs centres de traitement réparties dans le monde ce qui permet une reconfiguration réseau facile. La sécurité de l'utilisation de la console devient impérative par des procédés comme l'authentification multi facteurs ou par connexion chiffrée.

b. Service de stockage de données

Le service de stockage de données est un élément de la sauvegarde des données dans le cloud. Les constructeurs recopient les données dans différents centres pour permettre la redondance de celles-ci et permettre une restauration rapide. Si le contenu doit rester confidentiel, il va falloir une procédure de chiffrement de ces données avant leur stockage.

c. Infrastructure de calcul

Un des avantages du cloud pour le développement d'applications réside dans virtualisation. L'un des gros problèmes est la sécurisation des applications partagées, cette sécurité est garantie par l'hyperviseur donc il va falloir s'assurer que l'hyperviseur dispose des dernières mises à jour.

d. Services de support

La principale caractéristique de cloud est la mise en place a priori d'une sécurité renforcée avec des possibilités d'audits par des processus d'authentification, logs, pare-feu etc.

Il faut donc traiter les risques liés à l'intégration des applications des utilisateurs.

e. Sécurité périmétrique du réseau cloud

Les infrastructures cloud fournissent généralement des systèmes de protections contre DDoS (Distributed Denial of Service). Cela au travers de WAF (Web Application Firewall).

2.2 Les problèmes de sécurité liés aux conteneurs

Les problèmes de sécurité essentielles liés aux conteneurs sont :

- Afflux de codes sources vulnérables

Les conteneurs constituent une plateforme open source utilisée par les développeurs pour mettre à jour régulièrement et stocker des images dans des dépôts. Le fait de manipuler plusieurs codes source d'origine divers qui peuvent inclure des vulnérabilités peut donc compromettre la sécurité de tout le système.

- Grande surface d'attaque

Les systèmes hébergés dans le cloud sont constitués de plusieurs conteneurs, machines virtuelles, bases de données cela crée une grande surface d'attaque car nous avons affaire à plusieurs vulnérabilités d'origine divers ce qui accroît la difficulté à détecter les attaques.

- Manque de visibilité

Le moteur de conteneur est connecté et interfacé avec le noyau de linux ce qui crée une autre couche d'abstraction dans le fonctionnement des conteneurs cela rend difficile le suivi d'activités liées aux conteneurs et même aussi cela complique le suivi des activités des utilisateurs qui utilisent ces dits conteneurs.

- Compromission de secrets

Les conteneurs ont besoins d'informations sensibles comme : les clés d'API, identifiants et mots de passes pour accéder à un service. Si un pirate a accès illicitement à ces informations il peut les utiliser pour compromettre la sécurité de tout le système.

- **Vitesse dans le DevOps**

Les conteneurs peuvent être exécuter rapidement puis être arrêter et supprimer. Cette furtivité peut être exploité par des personnes malveillantes qui peuvent lancer une attaque et se cacher par les conteneurs sans installer un code.

- **Perturbation de conteneur voisin**

Un conteneur peut consumer toutes les ressources disponibles du système cela affecte automatiquement les opérations des conteneurs voisins ce qui créer une attaque par déni de service.

- **Fuite au niveau des conteneurs**

Un conteneur que l'on exécute en « root » peut être utiliser par un pirate pour passer la sécurité d'un autre conteneur pour y avoir accès à l'hôte hébergé par l'élévation de privilège. Ce qui permettra au pirate de passer l'isolation de tous les conteneurs.

- **Attaques au niveau réseau**

Un pirate peut exploiter un échec de connexion au niveau d'un conteneur qui a encore des sockets actifs et exploiter les connexions sortantes du réseau pour lancer des attaques sur le réseau.

- **Complexité de l'écosystème**

Les conteneurs sont conçus, gérer et déployer en utilisant les technologies de multiples vendeurs. Cela rend complexe la mise à jour des composants de manière individuel car ils sont originaires de plusieurs vendeurs.

2.3 Les 10 problèmes de sécurité du selon OWASP

OWASP (Open Web Application Security Project) est une communauté à but non lucratif mondialement connue dans le domaine de la sécurité des applications.

OWASP a présenté 10 risques courantes dans l'utilisation des technologies liées au cloud.

- **Risque 1 : responsabilité dans la gestion des données**

Le fait d'utiliser un cloud public pour gérer les données d'une entreprise accroît le risque d'exposition des données de l'entreprise par rapport à un datacenter classique. Avec certaines technologies du cloud nous perdons la responsabilité de la gestion de nos données.

- **Risque 2 : problème de fédération des identités**

Les entreprises utilisent des services et des applications de différents fournisseurs de services cloud. Ils créent donc plusieurs comptes chez ces différents fournisseurs ce qui complique la gestion des identités.

- **Risque 3 : problème de réglementation**

La réglementation liée à la sécurité des données peut varier d'un pays à un autre. Cela rend la gestion juridique complexe en termes de transparence et de lois.

Par exemple sur tout territoire de l'union européenne la réglementation liée à la protection des données est régie par le RGPD (Règlement Général de Protection des Données).

Dans ce même ordre la protection des données hospitalières aux USA est gérée par le HIPAA (Health Insurance Portability Accountability Act).

- **Risque 4 : résilience et continuité de l'activité**

Le fait d'avoir recours à un fournisseur de service cloud pour la continuité de l'activité en cas de désastre pose un risque en cas de mauvaise gestion du désastre par le fournisseur de services cloud en cas de désastre ce qui peut provoquer une perte financière à l'entreprise.

- **Risque 5 : confidentialité et second usage des informations**

L'utilisation des réseaux sociaux pose un problème de réutilisation des données personnelles des utilisateurs par les opérateurs de réseaux sociaux situés dans cloud.

- **Risque 6 : service et intégration de données**

Les entreprises doivent s'assurer de la sécurisation des transferts des données personnelles entre l'entreprise et le fournisseur de services cloud. Une non sécurisation du canal peut résulter à une interception de données par quelqu'un de malveillant.

- **Risque 7 : localisation multiple**

Le concept de localisation multiple permet de permet des données entre multiple clients.

Un mauvais cloisonnement logique des accès aux données pout résulter une interférence au niveau **des** règle de sécurité.

- **Risque 8 : Réponse aux incidents et rapport forensiques**

Lors des audits, les auditeurs peuvent être confronter à la multiple location des données recueillies dans le journal des évènements.

- **Risque 9 : Sécurité de l'infrastructure**

Une mauvaise configuration au niveau du déploiement de l'infrastructure peut provoquer des failles de sécurité comme le scan de ports en vue de la découverte de ports ouverts et même la découverte de mot de passe usuel utilisé lors de la configuration peut être un problème majeur de sécurité.

- **Risque 10 : exposition d'un environnement de test**

L'exposition d'un environnement de test peut résulter en des tentatives d'accès non autorisé.

-

3. Les principales attaques sur le cloud

L'objet de cette partie est de présenter les différentes attaques connues sur le cloud.

3.1 Attaque sur le canal cloud

Dans cette attaque, le pirate place une machine virtuelle malicieuse dans le même réseau physique où se trouve la machine virtuelle de la victime dans le but de voler des informations comme les clés cryptographiques de la victime.

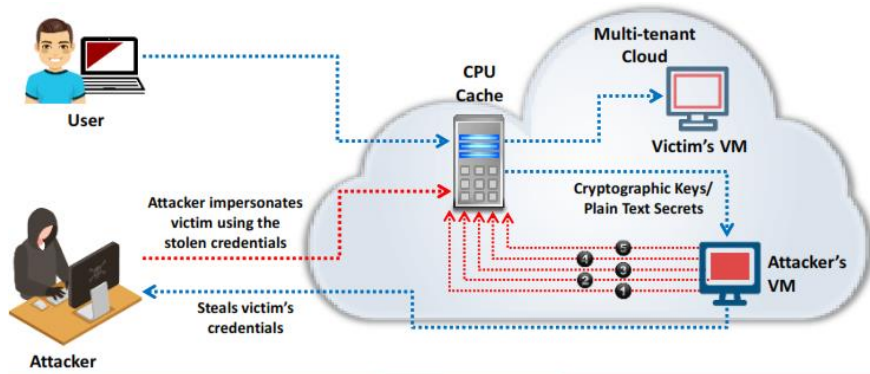


Figure 3

Comme contre mesure il est conseillé d'installer un pare feu virtuel afin de protéger l'infrastructure. Il faut aussi implémenter un processus de cryptographie aléatoire.

Le verrouillage des images des systèmes d'exploitation et des instances d'application permettent de lutter contre cette attaque.

3.2 Attaque sur l'emballage des messages

Cette attaque est effectuée par le pirate lors de la translation des messages SOAP dans la couche TLS (Transport Layer Security).

SOAP (Simple Object Access Protocol) est un protocole de communication basé sur XML pour permettre aux applications de s'échanger des informations via HTTP. Il permet ainsi l'accès aux services web et l'interopérabilité des applications à travers le web.

Le pirate duplique le corps du message et l'envoi au serveur comme un utilisateur légitime.

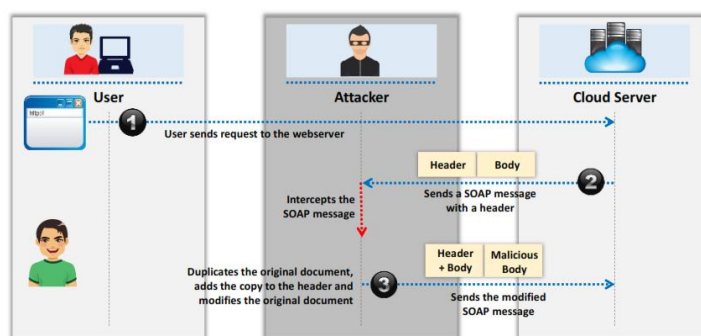


Figure 4

Pour lutter contre cette attaque, il faut mettre en place un processus de validation de schéma XML afin de permettre de détecter les messages SOAP. Appliquer le cryptage des authentifications sur les spécifications XML.

3.3 Attaque par homme du milieu dans le cloud

L'attaquant trompe la victime en lui faisant installer un code malicieux sur sa machine. Ce code malicieux permettra au pirate de voler le jeton de synchronisation au drive de la victime dans le cloud.

Après l'accès malicieux au drive de la victime le pirate restaure le jeton de synchronisation de la victime ce qui permet de remettre les applications de la victime utilisées par le pirate dans leur état initial.

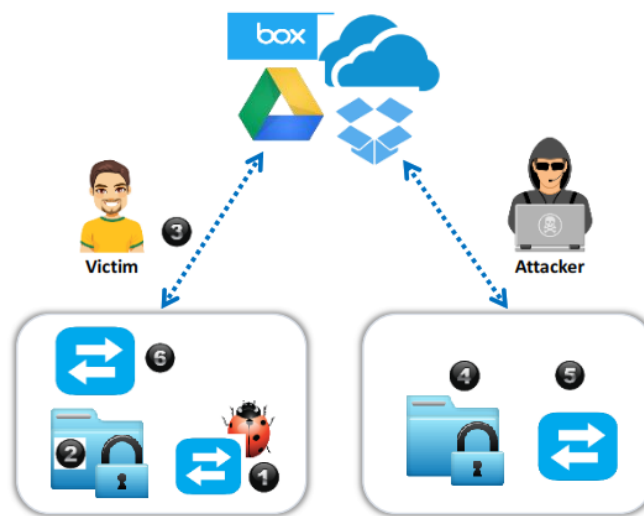


Figure 5

Il est conseillé comme contre mesure liée à cette attaque d'utiliser une passerelle de sécurité des emails afin de détecter les attaques par ingénierie sociale. Mais surtout de renforcer les règles de sécurité liées à l'expiration des jetons. Enfin il est recommandé d'implémenter un CASB (Cloud Access Security Broker) afin de surveiller le Traffic.

Un Cloud Access Security Broker (CASB) est un outil ou un service logiciel qui se situe entre l'infrastructure sur site d'une organisation et l'infrastructure d'un fournisseur de services Cloud. Le CASB est un gardien et permet à l'organisation d'étendre la portée de ses politiques de sécurité au-delà de sa propre infrastructure.

CASB offrent généralement les services suivants :

- Pare-feu (Firewall) pour identifier les logiciels malveillants (Malware) et les empêcher d'entrer sur le réseau de l'entreprise.
- Authentification pour vérifier les identifiants des utilisateurs et s'assurer qu'ils n'accèdent qu'aux ressources appropriées de l'entreprise.
- Pare-feu d'applications Web (WAF) pour contrecarrer les programmes malveillants conçus pour violer la sécurité au niveau des applications, plutôt qu'au niveau du réseau.
- La prévention des pertes de données (DLP – Data Loss Prevention) pour s'assurer que les utilisateurs ne peuvent pas transmettre des informations sensibles en dehors de l'entreprise.

3.4 Attaque par hameçonnage dans le cloud

Dans cette attaque le pirate envoie d'un mail d'hameçonnage incluant un code malicieux dans l'optique de récupérer les identifiants et les mots de passe des utilisateurs légitimes enfin d'avoir accès des documents confidentiels de l'entreprise.

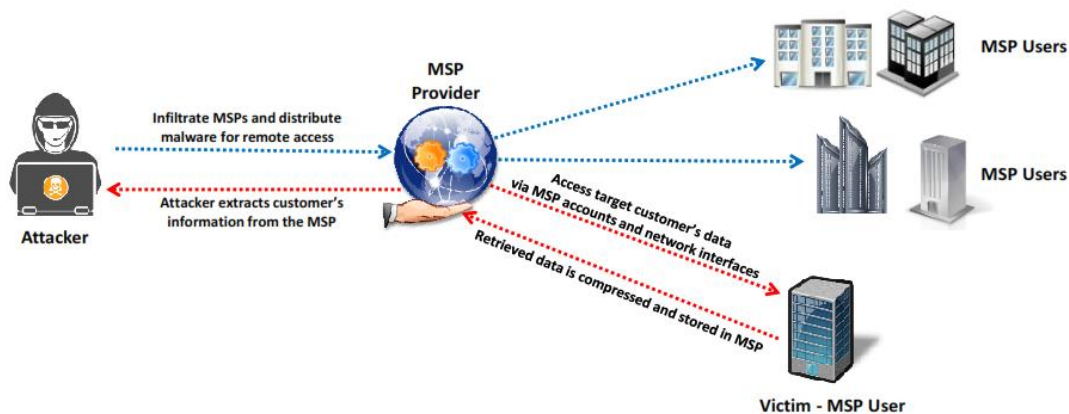


Figure 6

Pour contrer carrer cette parade il est recommandé d'implémenter une authentification multi facteurs.

Former les utilisateurs aux règles de sécurité liées au service cloud.

3.5 Attaque par vol de crypto monnaie

Le « cloud cryptojacking » exploite la mauvaise configuration des services cloud pour avoir des gains sur les bitcoins de la victime. Elle implique un pirate et un complice dans l'organisation.

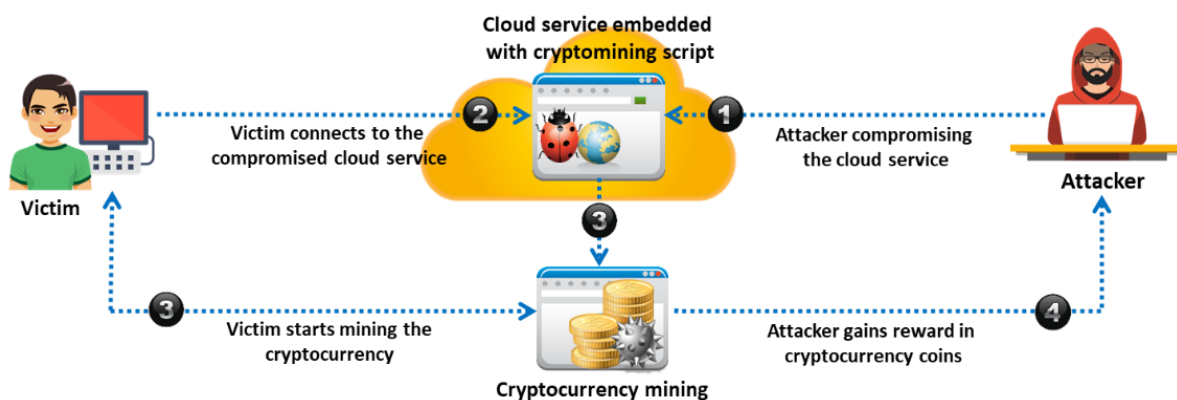


Figure 7

Pour lutter contre cette menace, il faut mettre premièrement en place une politique solide de mot de passe. En deuxième position il faut préserver différentes copies de vos données dans différents endroits et surtout une copie hors site.

En troisième position installer un « coinblocker URL » qui est un logiciel qui protège les utilisateurs contre les attaques de minage de pièces basées sur le navigateur. En plus de la liste noire et de la liste blanche des domaines, il prend également en charge l'analyse JavaScript avancée pour identifier et bloquer les fonctions JavaScript malveillantes. L'extension peut également identifier et bloquer les publicités malveillantes chargées dans les iframes par des publicités tierces.

3.6 Attaque sur le firmware des serveurs cloud

C'est une attaque qui exploite la structure des puces pour écrire dans le « firmware » du serveur en « bare-metal ».

Un firmware (ou logiciel embarqué en français) est un programme informatique intégré dans un matériel, qui participe à son bon fonctionnement et qui lui permet d'évoluer (via l'installation de mises à jour) sans avoir besoin de remplacer ce matériel ou de revoir son design.

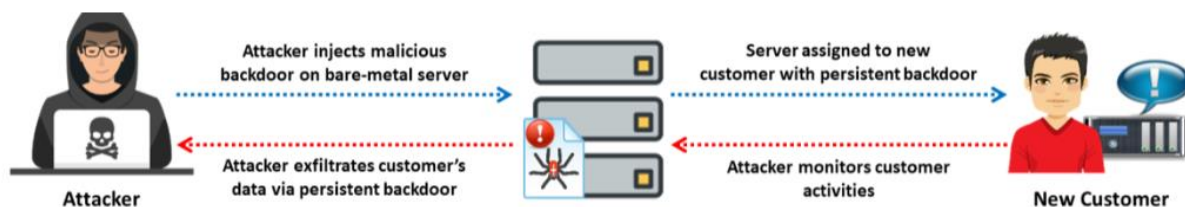


Figure 8

Afin d'éviter cette attaque, il faut maintenir le firmware à jour et faire des vérifications avant de les utiliser.

Bibliographie

- [1] Virtualisation en pratique, Kenneth Hess, Amy Newman, Pearson Education France 2010.
- [2] Citrix Xenapp 5, concepts et mise œuvre de la virtualisation d'applications, Sylvain Gaumé, Eni Editions 12 janvier 2009.
- [3] Cloud computing, sécurité et gouvernance du SI hybride et panorama du marché, Guillaume Plouin, 4^{ème} edition, dunod 2016.
- [4] Cloud computing – Informatique en nuage, Jean-Paul Figer, techniques de l'ingénieur, Technologies de l'information, Technologies logicielles, Architectures des systèmes, 10 février 2012.
- [5] Ethical Hacking Essentials Version 1 EC-COUNCIL 2021