CAHIERS AFRICAINS DES DROITS DE L'HOMME ET DE LA DÉMOCRATIE AINSI QUE DU DÉVELOPPEMENT DURABLE
REVUE AFRICAINE INTERDISCIPLINAIRE

ISSN : 2791-1063 (Imprimé)
ISSN : 2791-1071 (En ligne)

Numéro 73 - Volume 2 - Octobre-Décembre 2021

PROBLÉMATIQUE SUR LA SÉCURITÉ DES RÉSEAUX INFORMATIQUES À L'ÈRE DU CLOUD COMPUTING

Par

Héritier BUEYA MAVANGA et Samuel TSHIMPOLO TSHITOKONGO
Assistants à l'Institut Supérieur Pédagogique de Kangu à Tshela

RÉSUMÉ

Ces dernières années, il est difficile, voire impossible d'imaginer son quotidien en occultant l'informatique. Les possibilités offertes par ce domaine sont vastes et facilitent grandement notre quotidien ainsi que celui des entreprises. Les ordinateurs portables, smartphones et tablettes nous permettent d'être connectés à chaque instant, peu importe notre localisation. Cette mobilité couplée à cette connexion « permanente » ouvre un spectre offrant une multitude de possibilités.

Le monde de l'informatique est en constante évolution, caractéristique qui le rend d'autant plus fascinant. Les innovations, révolutions et autres changements majeurs sont légions dans ce domaine qui ne cessent d'évoluer.

*Ainsi, la demande croissante pour de nouveaux services informatiques plus économiques a permis l'émergence d'une nouvelle architecture qu'est le **Cloud Computing** (informatique dans les nuages), une manière différente d'utiliser les ressources informatiques à notre disposition.*

Le Cloud Computing représente la cinquième génération de l'informatique après les mainframes, les ordinateurs personnels, le paradigme client/serveur et le web (World Wide Web). Il désigne un modèle dans lequel les ressources telles que la puissance de calcul, le stockage ou encore la bande passante sont fournies comme des services qui peuvent être loués par des utilisateurs via Internet à la demande.

Cette technologie offre plusieurs avantages comme un déploiement rapide, un paiement à l'usage, une réduction de coûts, une évolutivité facile, une délivrance de service plus rapide, un accès au réseau omniprésent, une plus grande résilience, etc. en raison de ces diverses caractéristiques, il devient une solution intéressante pour les entreprises et les chercheurs[1].

[1] *Etat de l'Art Cloud Computing.* Livre blanc par SOGETI Enterprise Services Consulting Mars 2009.

Cependant, son adoption est confrontée à un certain nombre de défis, tels que les problèmes de sécurité, les défis juridiques et de conformité et les défis organisationnels. Tous ces défis présentent un élément commun qui est la problématique de sûreté entre les consommateurs et les fournisseurs, puisque le Cloud Computing exige de faire confiance aux fournisseurs sur la gestion des ressources informatiques et l'administration des données. En conséquence, la confiance représente l'un des principaux freins pour l'adoption de ce nouveau paradigme.

INTRODUCTION

Le réseau Internet se développe de manière exponentielle depuis sa création. L'intensification de son utilisation est possible grâce à l'augmentation continue des capacités de calcul, de stockage et de débit. Dans ce contexte, la notion de service informatique s'est également fortement développée ces dernières années, que ce soit pour les particuliers ou les professionnels.

Afin d'assurer ces services, les systèmes répartis sont aujourd'hui prédominants. Le paradigme du Cloud Computing est depuis quelques années en train de prendre une place centrale pour la délivrance et la consommation de services, comme le montrent plusieurs études. Le Cloud Computing permet à des utilisateurs de consommer des ressources informatiques en tant que services de différentes natures, avec différents niveaux de contrôle sur les technologies utilisées. Les ressources proposées comprennent des infrastructures, des plateformes de développement et d'exécution ou des applications. Elles sont généralement hébergées chez un fournisseur de services. Un des objectifs principaux du modèle cloud est de permettre aux clients de réduire les coûts de déploiement et d'opération de ressources qui étaient hébergées traditionnellement dans leurs locaux[2].

Aux bénéfices du modèle cloud sont associés des problématiques de sécurité, comme dans tout système informatique réparti.

La diversité des acteurs mêlée à la variété des technologies dans le cloud implique un grand nombre de menaces et rend la sécurisation des données complexe. Pour prévenir et détecter les attaques, des mécanismes de sécurité réseau sont déployés dans le cloud.

[2] Vincent Nicomette, Mohamed Kaâniche, Eric Alata et Matthieu Herrb, Set-Up and Deployment of a High-Interaction Honeypot : Experiment and Lessons Learned. Journal in Computer Virology, 2011.

Nous nous intéressons au contrôle d'accès réseau assuré par les pare-feu. Or, il n'est pas aisé pour les administrateurs de déployer correctement ces outils de sécurité sans perturber le fonctionnement du cloud. Il est donc essentiel de rechercher régulièrement les faiblesses, déviances ou incohérences dans le déploiement de ces outils.

1. LA SÉCURITÉ RÉSEAU[3]

Aujourd'hui, la plupart d'organisations dépendent largement des réseaux informatiques pour partager des informations de manière efficace et productive au sein du réseau défini. De nos jours, les réseaux informatiques organisationnels sont très vastes, en supposant que chaque membre du personnel dispose d'un poste de travail dédié. Une grande entreprise aurait des milliers de postes de travail et de serveurs sur le réseau.

Il est probable que ces postes de travail ne soient pas gérés de manière centralisée ou qu'ils aient des paramètres de protection appropriés. Les organisations peuvent avoir une variété des systèmes d'exploitation, des matériels, des logiciels et des protocoles avec différents niveaux de cyber-conscience parmi les utilisateurs. Imaginez que ces milliers de postes de travail sur les réseaux d'entreprise soient directement connectés à Internet. Ce type de réseau non sécurisé contenant des informations sensibles et des données précieuses deviendra la cible d'une attaque. La sécurité du réseau aide à résoudre ces problèmes.

La sécurité du réseau se compose de politiques et de pratiques adoptées pour empêcher et surveiller l'accès non autorisé, la modification abusive ou le refus d'un réseau informatique et d'accéder aux ressources du réseau. L'autorisation d'accès aux données dans un réseau est prise en charge par la sécurité du réseau, qui est contrôlée par l'administrateur réseau ou l'ingénieur de sécurité réseau.

La sécurité du réseau couvre également les transactions et les communications entre les entreprises, les agences gouvernementales et les particuliers. Les réseaux peuvent être privés, comme au sein de l'entreprise, ou être ouverts au public et la sécurité est impliquée dans les deux couches. Il sécurise le réseau ainsi que protège et supervise les opérations effectuées sur le réseau.

[3] https://geekflare.com/fr/learn-network-security/

Voici quelques-uns des différents types de sécurité réseau :

- ✓ Les pare-feu ;
- ✓ Sécurité du courrier électronique ;
- ✓ Antivirus/Antimalware ;
- ✓ Segmentation du réseau ;
- ✓ Contrôle d'accès ;
- ✓ Sécurité des applications ;
- ✓ Prévention des pertes de données ;
- ✓ Détection de la prévention des intrusions ;
- ✓ Sécurité sans fil ;
- ✓ Sécurité Web ;
- ✓ VPN ;
- ✓ Sécurité sans fil.

2. LE CLOUD COMPUTING

Le Cloud Computing est une métaphore de l'Internet, provenant de sa représentation commune dans les diagrammes réseau (ou plus généralement des composants qui sont gérés par d'autres) comme nuages.

Ce concept remonte à 1960 lorsque John McCarthy a estimé que « le calcul pourrait un jour être organisé comme une entreprise de service public ».

Le Cloud Computing, aujourd'hui utilisé largement dans le langage courant, est un modèle d'accès à travers le réseau Internet à un ensemble de ressources numériques, pouvant être allouées et libérées à la demande et pour lesquelles le fournisseur du service assure l'ensemble des activités de maintenance, de support et d'exploitation, c'est-à-dire, il consiste à accéder à des données et des services sur un serveur distant.

Ce modèle offre des services de différentes natures, allant des services d'infrastructure (location de capacités de stockage ou de calcul), des services de plateforme (location d'environnements de développement préconfigurés) ou de services d'applications (location d'applications).

Traditionnellement, une entreprise utilisait sa propre infrastructure pour héberger ses services. Elle achetait donc ses propres serveurs et assurait le développement et la maintenance des systèmes nécessaires à son fonctionnement.

Par opposition, le Cloud Computing se repose sur une architecture distante, Le fournisseur donc assure la continuité du service et de la maintenance. Les

services de Cloud Computing sont accessibles via un navigateur web. Le terme Cloud Computing étant anglais, on retrouve comme synonymes les termes suivant : informatique virtuelle, informatique dans les Cloud et informatiques en Cloud ou encore informatique dématérialisée. L'emplacement des données dans le Cloud n'est pas connu des clients, ceux-ci ont simplement l'accès à la partie applicative, sans se soucier du reste[4].

2.1. Terminologie générale[5]

Le monde informatique contient des milliers d'abréviations et d'acronymes tous plus obscurs les uns que les autres et le Cloud Computing n'échappe pas à la règle. Le monde du Cloud Computing est littéralement noyé sous les abréviations et les acronymes dont certains ont même plusieurs sens.

- ✓ **CAAS :** Plusieurs significations différentes de CAAS sont utilisées comme : Capability as a Service, Communication as a Service, Cloud as a Service, Computing as a Service, Content as a Service, Community as a Service, Car as a Service. Toutefois, la plupart des gens s'accordent pour dire que le CAAS correspond bien à (Communication as a Service). Le CAAS consiste à fournir des moyens de communication en tant que service, via Internet.
- ✓ **SAAS :** L'acronyme « SAAS » est le plus connu dans le monde du Cloud Computing. Sa signification est « Software as a Service », autrement dit, application en tant que service, c'est un modèle de déploiement d'application dans lequel un fournisseur loue une application clé en main à ses clients en tant que service à la demande au lieu de leur facturer des licences.
- ✓ **PAAS :** Le PAAS qui signifie « Platform as a Service » est une architecture composée de tous les éléments nécessaires pour soutenir la construction, la livraison, le déploiement et le cycle de vie complet des applications et des services exclusivement disponibles à partir d'internet. Elle est également connue sous le nom de « CloudWare ». Le PAAS offre des facilités à gérer le déroulement des opérations lors de la conception, du développement, du test, du déploiement et de l'hébergement d'applications web à travers des outils et des services tels que :
  - Le travail collaboratif (« team collaboration ») ;

[4]] http://www.partagedefichier.com/blog/cloud-computing-definition/ Juin 2012.
[5] N. Grevet. Le cloud computing : évolution ou révolution ? Pourquoi, quand, comment et surtout faut-il prendre le risque ? Août 2009.

- L'intégration des services web et bases de données. Ces services sont fournis au travers une solution complète destinée aux développeurs et disponible immédiatement via l'internet.

✓ **L'IAAS (Infrastructure as a Service)** est un modèle qui permet de fournir des infrastructures informatiques en tant que service. Ce terme était originellement connu sous le nom de (Hardware as a Service).Ces infrastructures virtuelles composent un des domaines du « As a Service » en empruntant la même philosophie de fonctionnement et de tarification que la plupart des services du Cloud Computing.

Plutôt que d'acheter des serveurs, des logiciels, et l'espace dans un centre de traitement de données et/ou de l'équipement réseau, les clients n'ont plus qu'à louer les ressources auprès des prestataires de service. Le service est alors typiquement tarifé en fonction de l'utilisation et de la quantité des ressources consommées. De ce fait, le coût reflète typiquement le niveau d'activité de chaque client. C'est une évolution de l'hébergement Internet qui se différencie des anciens modes de fonctionnement, on distingue :

✓ **Hébergement mutualité** : une machine pour plusieurs clients, gérée par un prestataire de service et dont les clients payent le même prix peu importe leur utilisation.

✓ **Hébergement dédié :** une machine pour un client, gérée le plus souvent par le client lui-même et pour laquelle le client paye le même prix chaque mois peu importe son utilisation.

✓ **Infrastructure as a Service :** un nombre indéfini de machines pour un nombre indéfini des clients, dont les ressources sont combinées et partagées pour tous les clients. Chaque client paye en fonction de son utilisation de l'architecture.

2.2. Types de Cloud Computing

Le concept de Cloud Computing est encore en évolution. On peut toutefois citer quatre types de Cloud Computing[6] :

✓ **le Cloud privé** (ou interne) : c'est un réseau informatique propriétaire ou un centre de données qui fournit des services hébergés pour un nombre limité d'utilisateurs ;

[6] V. Kherbache, M. Moussalih, Y. Kuhn, A. Lefort, *Cloud Computing*, IUT Nancy Charlemagne.2009/2010.

- ✓ **le Cloud public** (ou externe) : C'est un prestataire de services qui propose des services de stockage et d'applications Web pour le grand public. Ces services peuvent être gratuits ou payants ;
- ✓ **le Cloud hybride** (interne et externe) : C'est un environnement composé de multiples prestataires internes et externes ;
- ✓ **« Multi-cloud[7] »** signifie plusieurs clouds publics. Une entreprise qui utilise un déploiement multi-cloud intègre plusieurs clouds publics de plusieurs fournisseurs de cloud. Au lieu d'une entreprise utilisant un seul fournisseur pour l'hébergement cloud, le stockage et la pile d'applications complète dans une configuration multi-cloud, elle en utilise plusieurs. Les déploiements multi-cloud ont un certain nombre d'utilisations.

Un déploiement multi-cloud peut tirer parti de plusieurs fournisseurs IaaS (Infrastructure-as-a-Service), ou il peut utiliser un fournisseur différent pour IaaS, PaaS (Platform-as-a-Service) et SaaS (Software-as-a- services). Le multi-cloud peut être purement à des fins de redondance et de sauvegarde du système, ou il peut incorporer différents fournisseurs de cloud pour différents services. La plupart des entreprises qui migrent vers le cloud se retrouveront avec une sorte de déploiement multi-cloud. Un déploiement multi-cloud peut même se produire involontairement, en raison du shadow IT.

2.3. Avantages du Cloud Computing

Les avantages du Cloud Computing sont :

- ✓ **Souplesse d'évolution :** il n'y a pas de logiciel à installer et l'accès se fait avec un simple navigateur web.
- ✓ **Simplicité :** l'entreprise cliente n'a plus besoin de développements coûteux et déplace la responsabilité du fonctionnement du service sur le fournisseur.
- ✓ **Liberté de changement de service :** le Cloud Computing étant généralement facturé à la demande ou par abonnement mensuel, il est très facile pour une entreprise d'arrêter le service si elle n'en a plus besoin ou si elle souhaite aller chez un concurrent.
- ✓ **Coût :** la force du Cloud Computing réside dans la possibilité de proposer le même service à un grand nombre d'utilisateurs, finalement, le coût de Cloud Computing sera donc très raisonnable.
- ✓ Bas-coût d'ordinateurs, d'infrastructure et de softwares.
- ✓ Rendements élevés.
- ✓ Capacité de stockage illimitée.

[7] https://www.cloudflare.com/fr-fr/learning/cloud/what-is-multicloud/

- ✓ Peu d'entretien.
- ✓ Mises à jour instantanées de logiciel.
- ✓ Sûreté accrue de données.
- ✓ Une collaboration plus facile de groupe.
- ✓ Accès universel aux documents

2.4. Inconvénients du Cloud Computing

Les inconvénients du Cloud Computing sont :

- ✓ **Confidentialité et sécurité des données :** les données sont hébergées en dehors de l'entreprise. Les fournisseurs proposant le service héberge des données d'entreprise utilisatrice, Cela peut donc poser un risque potentiel pour l'entreprise de voir ses données mal utilisées ou volées. Il s'agit donc d'assurer que le fournisseur dispose d'une sécurité suffisante et qu'il propose une politique de confidentialité concernant les données d'utilisateur.
- ✓ **Dépendance:** si l'entreprise souhaite des fonctionnalités très spécifiques, il peut être difficile de convaincre le fournisseur de proposer ces fonctionnalités. Et en général, s'il y a un problème, l'entreprise est tributaire du service client d'un fournisseur. Il s'agit donc de choisir un fournisseur en qui l'on a confiance.
- ✓ Besoin d'un raccordement constant d'Internet.
- ✓ Exige une grande largeur de bande.
- ✓ Peut-être plus cher pour certain cas d'utilisation.

3. LES TRAVAUX CONNEXES SUR LA SÉCURITÉ DU CLOUD

Il existe plusieurs travaux réalisés dans ce domaine.

- ✓ **SATISH et ANITA**[8], ont proposé une méthode de faux écran pour assurer l'authentification à deux niveaux dans le cloud computing.
- ✓ **ARASU et AL.**[9]**,** ont proposé une méthode utilisant le code d'authentification de message dans laquelle la clé cryptographique, le message et la fonction de hachage sont concaténés ensemble pour assurer l'authentification.

[8] K. Satish and G. Anita, "Multi-Authentication for Cloud Security: A Framework," Int. J. Comput. Sci. Eng. Technol. IJCSET, vol. 5, no. 04, Apr. 2014.

[9] A.S. Ezhil, G. B, and A. S, "Privacy -Preserving Public Auditing In Cloud Using HMAC Algorithm," Int. J. Recent Technol. Eng. IJRTE, vol. 2, Mar. 2013.

- ✓ **PARSI et SUDHA**[10], ont proposé une méthode utilisant l'algorithme RSA pour l'authentification et le transfert sécurisé de données. Cette méthode implique une phase de génération de clé, le chiffrement et le déchiffrement.
- ✓ **BALASARASWATHI et MANIKANDAN**[11]**,** ont proposé une architecture de cloud multiple basée sur le partitionnement de données chiffrées avec une approche dynamique afin de sécuriser l'information en transit ou en reste. Nous avons analysé plusieurs approches de transfert sécurisé de données, ces approches se focalisent principalement sur les paramètres d'authentification. En effet, les données en transit vers le cloud peuvent être attaquées par différents intercepteurs non autorisés. Une méthode particulière ne suffit pas à traiter toutes les questions de sécurité et de confidentialité des données. Par conséquent, différentes techniques et mécanismes intégrés devraient être utilisés[12].

4. LA SÉCURITÉ RÉSEAU À L'ÈRE DU CLOUD COMPUTING[13]

Auparavant, les organisations stockaient leurs données sur site. Ils avaient leur propre entrepôt. Désormais, la majorité d'organisations passent au Cloud.

Le cloud computing transforme la façon dont nous faisons des affaires, rendant l'informatique plus efficace et plus rentable. Mais il ouvre également les entreprises à de nouveaux types de cybermenaces. Si un pirate informatique peut accéder aux réseaux via le cloud, les organisations peuvent être gravement endommagées. C'est une menace qui ne fait qu'augmenter. Même le risque que des pirates informatiques volent des données a augmenté de façon exponentielle.

Par conséquent, la sécurité du cloud est très cruciale et la sécurité du réseau en fait partie. Le cloud computing a très certainement été un moteur important pour la prochaine génération d'Internet. Cette technologie clé a facilité à la fois le stockage en ligne dans le cloud et, plus récemment encore, les services en

[10] P. Kalpana and S. Singaraju, "Data security in cloud computing using RSA algorithm," IJRCCT, vol. 1, no. 4, pp. 143–146, 2012.
[11] V. R. Balasaraswathi and S. Manikandan, "Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach," in Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on, 2014, pp. 1190–1194.
[12] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, "Securing elastic applications on mobile devices for cloud computing," 2009, p. 127.
[13] https://www.hebergementwebs.com/vpn/qu-est-ce-que-la-securite-des-reseaux-a-l-ere-du-cloud-computing

ligne, permettant aux applications Software as a Service (SaaS) disponibles par abonnement.

Alors que le cloud computing a été un formidable catalyseur pour ces services, il a également présenté de nouveaux défis pour sécuriser un réseau. Il est loin le temps où le service informatique d'une entreprise pouvait configurer des ordinateurs, puis contrôler l'intégralité du trafic - entrant et sortant - via son réseau organisé avec des pare-feux, des concentrateurs et un logiciel antivirus stratégiquement placés protégeant les clients.

Au contraire, avec le cloud computing, il existe des ressources virtuelles fournies sur Internet, notamment des données, des applications et des infrastructures. Cela peut alors exposer des données sensibles lorsqu'elles sont transmises du client au serveur cloud et vice-versa.

✓ **Vulnérabilités modernes du réseau**

Une vulnérabilité courante du cloud computing est connue sous le nom de détournement de session. Dans ce type d'attaque, le pirate exploite une session informatique valide, pour ensuite accéder aux ressources du fournisseur de serveur cloud.

Ici, le cookie que le client utilise pour l'authentification de la session valide obtient volé et détourné. Dans une variante de l'attaque, le pirate intercépte le trafic entre le client et le serveur avec un «programme de reniflement», qui peut récupérer le cookie (et toutes les autres données) dans ce qui est appelé une « attaque d'homme au milieu».

✓ **Stratégies et solutions de sécurité**

Plusieurs stratégies ont été développées pour assurer la sécurité entre les clients et le serveur cloud. Ils doivent être adaptés au type spécifique de plate-forme de sécurité cloud qui est vulnérable. La base de l'architecture cloud est connue sous le nom d'Infrastructure as a Service (IaaS). À protect IaaS, il doit y avoir une segmentation du réseau et la surveillance du réseau doit inclure les systèmes de détection des intrusions (IDS) et les systèmes de prévention des intrusions (IPS). Il devrait également y avoir des pare-feu d'applications Web virtuelles situés en face du site Web pour la protection contre les logiciels malveillants. Les routeurs virtuels et les pare-feux basés sur le réseau virtuel le long du bord du réseau cloud offrent une protection de périmètre.

La prochaine solution cloud est Platform as a Service ou PaaS. Dans cette architecture, le fournisseur de services fournit au client la plate-forme qui lui

permet de créer des applications, tandis que l'entreprise hôte, c'est-à-dire: le fournisseur de cloud, construit et entretient l'infrastructure. La sécurité pour ce type de service cloud peut être assurée via des restrictions IP et la journalisation. En outre, des passerelles API doivent être déployées et un courtier de sécurité d'accès au cloud (CASB) qui contrôle les politiques.

Avec un SaaS, le logiciel et les données sont hébergés dans le cloud, avec le service disponible pour chaque utilisateur via un navigateur. La sécurité d'une telle configuration est souvent assurée via le fournisseur de services cloud (CSP), qui est généralement négocié dans le contrat de service. De plus, un SaaS incorporera la même suite de mesures de sécurité que dans un PaaS.

Une dernière mesure de sécurité à mettre en œuvre est un cloudVPN, également connue sous le nom de VPN en tant que service, ou bien désignée comme VPNaaS. Ce cloudVPN est conçu pour donner aux utilisateurs la possibilité d'accéder aux applications du serveur cloud via un navigateur en toute sécurité en chiffrant les communications.

5. DISCUSSION

Un **problème de sécurité** dans une plateforme sur le **cloud** peut engendrer une perte économique mais également une mauvaise réputation si toutefois cette plateforme est orientée vers un grand public. **Les problèmes de sécurité** du **cloud** sont la cause du retard de l'adoption massive de cette nouvelle solution[14].

Les problèmes de sécurité sont un domaine actif de recherche et d'expérimentation. Beaucoup de recherches sont en cours pour répondre aux problèmes tels que la sécurité des réseaux, protection des données, la virtualisation et l'isolement des ressources.

La sécurité ne consiste pas seulement à protéger votre identité et vos informations financières, bien que celles-ci soient importantes. Il est également essentiel pour préserver l'intégrité et l'accès à vos données et applications dans le cloud.

Des choses comme le pare-feu, le cryptage, les sauvegardes, l'isolation des ressources, la force de l'autorisation aux interfaces utilisateur et la sélection des employés et autres clients peuvent déterminer celui qui peut accéder à vos ressources, comment ils peuvent le faire et ce qu'ils peuvent faire.

[14] https://fr.wikipedia.org/wiki/Sécurité_du_cloud

Il y a beaucoup de choses perturbatrices qu'un intrus malveillant peut faire. Une attaque par déni de service qui consiste à bombarder un système au point où il est inaccessible pour une utilisation normale, peut rendre vos services de cloud temporairement indisponibles. Un compte piraté pourrait entraîner la redirection de vos données ou de vos transactions commerciales à des fins malveillantes ou la perte de l'accès à vos propres services.

Un système compromis pourrait permettre à une machine virtuelle hébergeant vos applications et vos informations d'être migrées vers un serveur malveillant, ce qui entraînerait une exposition d'informations et une perte éventuelle de données. Des logiciels malveillants (logiciels malveillants) peuvent infecter le système et perturber les opérations, voire compromettre votre ordinateur personnel ou professionnel s'il se répand. Même si une attaque ne vous fait pas perdre des données ou d'accès, toute violation de la sécurité diminuera probablement votre niveau de confort. Stocker ou récupérer des informations du Cloud.

Malheureusement, il n'y a pas de systèmes totalement infranchissables. Tout ce qui est accessible via Internet est vulnérable. Mais plus la sécurité d'un fournisseur de cloud est forte et plus sa capacité à détecter et à récupérer des violations est grande, moins vous risquez de perdre accès, de perdre vos données ou votre tranquillité d'esprit.

Et la sécurité ne dépend pas entièrement de l'hôte cloud. Les fautes personnelles, telles que succomber à une escroquerie par hameçonnage (où vous êtes trompés en donnant des informations de connexion) ou en téléchargeant des logiciels malveillants depuis une autre source peuvent également avoir des conséquences sur votre accès au cloud. La vigilance est requise de tous les côtés.

Répondre à ces problèmes, il faut obtenir la confiance de l'utilisateur pour les applications de cloud computing et des services. L'obtention de la confiance des utilisateurs peut être réalisée en créant la confiance de la ressource de cloud et les applications, ce qui est un problème crucial dans le cloud computing.

CONCLUSION

L'essor du Cloud Computing ces dernières années a entraîné le développement d'une multitude de services associés. Ces services concernent l'utilisation de ressources informatiques à distance : applications, plateformes de développement et d'exécution, infrastructures. Le modèle IaaS permet d'offrir aux clients du cloud des infrastructures virtuelles, généralement hébergées chez les fournisseurs de services. La dynamicité des environnements cloud, due au nombre de changements de configuration possibles par les clients et fournisseurs, peut impliquer des conséquences négatives sur la sécurité réseau du cloud. Pour se prémunir des menaces, ces infrastructures virtuelles sont protégées par des mécanismes de sécurité réseau comme les pare-feu virtuels et les systèmes de détection d'intrusion réseau. Les pare-feu ont pour rôle de gérer le contrôle d'accès réseau, tandis que les systèmes de détection d'intrusion doivent détecter les attaques survenant sur le réseau.

Le phénomène du Cloud Computing est inéluctable. Beaucoup de responsables informatiques se méfient de la gestion de la sécurité nécessaire pour le Cloud Computing. Toutefois, ces risques sont équilibrés par les avantages apportés par le Cloud Computing. Les économies de coûts est l'argument favorisée par les PDG et directeurs financiers et le responsable Sécurité aura à résoudre les différents risques liés à la sécurité du Cloud Computing. Le Cloud n'est pas une technologie nouvelle, mais une nouvelle façon de faire les choses en matière de technologie de l'information. Résister au changement est toujours difficile, des spécialistes de la sécurité de l'information auront à accompagner le développement du Cloud, afin de permettre à ses usagers de bénéficier de grands avantages que le Cloud offre.

BIBLIOGRAPHIE

I. OUVRAGES

1. Cloud Computing & SaaS de Guillaume Plouin, éditions Dunod, mars 2009.
2. PHILIPPON, G., *Mise en place d'un cloud privé et publique*, juillet 2014.
3. CASEIRO, Ph. et DEHHENNIN, D., *OpenNebula l'informatique élastique.*
4. NKIDIAKA, Ndongala Brady, *Intégration du Cloud Computing au sein d'une PME genevoise,* mai 2012.
5. NICOMETTE, V., KAÂNICHE, M., Eric ALATA, E. et HERRB, M., "Set-Up and Deployment of a High-Interaction Honeypot : Experiment and Lessons Learned", *Journal in Computer Virology*, 2011.
6. PANSANEL Jérôme, Installation OpenStack, juillet 2014.

II. WEBOGRAPHIE

1. Abicloud. Http://community.abiquo.com/. Consulté Avril 2021.
2. BOWERS K., JUELS A., OPREA A., HAIL: A High-Availability and Integrity Layer for Cloud Storage – Novembre 2009 RSA Laboratories. Consulté Novembre 2021.
3. Cloud Computing - Benefits and recommendations for information Security - November 2009. European Network and Information Security Agency (ENISA). Consulté Octobre 2021.
4. Clouds or storm clouds? Cloud Computing Security – May 2010 Security Acts issue. Consulté Août 2021.
5. CloudSecurity.org. Consulté Novembre 2021.
6. Diana Kelley," Cloud computing security model overview: Network infrastructure issues", http://searchcloudsecurity.techtarget.com/tip/, 2009. Consulté Février 2021.
7. Eucalyptus. http://www.eucalyptus.com/. Consulté Octobre 2021.
8. Frank Gens. Defining "Cloud Services" and "Cloud Computing". Septembre 2008. Disponible sur : http://blogs.idc.com/ie/?p=190. Consulté Octobre 2021.
9. Nimbus. http://www.nimbusproject.org/. Consulté Mars 2021.
10. Opennebula. http://opennebula.org/. Consulté Novembre 2021.
11. Robert McMillam. Cloud Computing est un « cauchemar de la sécurité » selon le PDG de Cisco. http://www.pcworld.com/article/163681/article.html, 2009. Consulté Septembre 2021.
12. SANTOS, N., GUMMADI, K., RODRIGUES, R., Towards Trusted Cloud Computing, 2010. Consulté Mars 2021.

13. Security Guidance for Critical Areas of Focus in Cloud Computing – April 2011. Cloud Security Alliance. Consulté Mai 2021.
14. TCG: http://www.trustedcomputinggroup.org. Consulté Mai 2021.
15. WINKLER, V., "Securing the Cloud : Cloud Computer Security Techniques and Tactics," Syngress 2011. Consulté Octobre 2021.