UNIVERSITÉ DU QUÉBEC EN OUTAOUAIS

THEME : Sécurité dans le Cloud

Objectif : Assurer la protection des données et des ressources hébergées dans des environnements de cloud computing, en identifiant et en atténuant les risques spécifiques au stockage, traitement et transmission de données dans le cloud.

Travail de session

Présenté à

Moudoud Hajar

Par

TAMBAT TRESOR MEGANE

Département d’informatique

CYB1003-01 : INTRODUCTION A LA CYBERSECURITE

Gatineau

4 DECEMBRE 2024

TABLE DES MATIÈRES

INTRODUCTION

La sécurité du cloud est un ensemble d'outils permettant de protéger les données et les autres informations numériques contre les menaces de sécurité, les erreurs humaines et les menaces internes. Elle a pour rôle d'atténuer les erreurs qui surviennent pendant le développement et de réduire le risque que des personnes non autorises accèdes a des données sensibles.de nos jour la question de sécurité des données et des ressources devient une priorité majeure pour les organisations .ce projet vise à aborder les différents défis de la sécurité tel que la protection des données et la réduction des vulnérabilités du cloud tout en proposant des stratégies de sécurité adapter au environnement cloud.

1- ARCHITECTURE DU CLOUD

1-1 Définition

La sécurité informatique dans le Cloud représente l'ensemble des technologies, protocoles et meilleures pratiques qui protègent les environnements informatiques dans le Cloud, les applications fonctionnant dans le Cloud ainsi que les données qui y sont stockées. La sécurisation des services dans le Cloud commence par connaître la nature exacte de ce qui est sécurisé ainsi que les aspects du système qui doivent être gérés.

En résumé, la conception de l'arrière-plan contre les vulnérabilités est en grande partie entre les mains des fournisseurs de services dans le Cloud. Outre le fait de choisir un fournisseur soucieux de la sécurité, les clients doivent avant tout correctement configurer le service et adopter des habitudes d'utilisation sûres. En outre, les clients doivent s'assurer que le matériel et les réseaux des utilisateurs finaux sont bien sécurisés.

Dans l'ensemble, la sécurité dans le Cloud est conçue pour protéger les éléments suivants, indépendamment de vos responsabilités :

- **Réseaux physiques** : routeurs, alimentation électrique, câblage, climatisation, etc.
- **Stockage des données** : disques durs, etc.
- **Serveurs de données** : matériel et logiciels de base pour les réseaux informatiques
- **Structures de virtualisation des ordinateurs** : logiciels de machines virtuelles, machines hôtes et machines invitées
- **Systèmes d'exploitation (SE)** : logiciels qui prennent en charge toutes les fonctions de l'ordinateur
- **Logiciel médiateur** : gestion de l'interface de programmation d'applications (API)
- **Environnements d'exécution** : exécution et maintenance d'un programme en cours d'exécution
- **Données** : toutes les informations stockées, modifiées et consultées
- **Applications** : services logiciels traditionnels (messagerie électronique, logiciels d'impôts, suites de productivité, etc.)
- **Matériel de l'utilisateur final** : ordinateurs, appareils mobiles, Object connectes, etc.

Dans le cas de l'informatique dans le Cloud, la propriété de ces composants peut varier considérablement. Cela peut rendre floue l'étendue des responsabilités des clients en matière de sécurité.

1-2 Historique

L'historique de la sécurité dans le cloud évolue en parallèle avec le développement du cloud computing. En résumé au début des années 1990-2000) l'origine, les préoccupations de sécurité concernaient principalement le cryptage des données en transit et la sécurisation des réseaux. Les systèmes étaient rudimentaires, se concentrant sur les pares-feux et les mécanismes d'authentification puis a suivi l'émergence des services cloud modernes de 2000-2010 avec l'arrivée d'AWS, Google Cloud et Microsoft Azure, la sécurité est devenue une priorité. Des protocoles comme SSL/TLS ont été adoptés pour sécuriser les communications, et les mécanismes d'accès basés sur les rôles (RBAC) ont commencé à être intégrés. En suite la Standardisation et réglementation de 2010-2020 caractériser par La montée des préoccupations en matière de confidentialité et de conformité (ex. RGPD, HIPAA) qui a poussé les fournisseurs de cloud à renforcer la sécurité. Des normes comme ISO 27001 et SOC 2 ont été établies. Les outils de gestion des identités (IAM) et le cryptage des données au repos sont devenus courants. Et enfin les Menaces modernes et solutions avancées de 2020 et au-delà elle se gère grâce à la sophistication des cyberattaques (ransomware, attaques par API), des solutions telles que l'intelligence artificielle pour la détection des intrusions, les architectures "zero trust" et le chiffrement homomorphique qui ont émergé. La sécurité dans les environnements multi-clouds et hybrides est devenue un défi majeur.[1]

1-3 Importance

L'importance de la sécurité dans le cloud repose sur plusieurs aspects essentiels [3]:

- Protection des données sensibles : Le cloud stocke des données critiques, souvent personnelles ou stratégiques.
- Gestion des menaces croissantes : Les cyberattaques sont de plus en plus sophistiquées et ciblent fréquemment les infrastructures cloud.
- Conformité réglementaire : De nombreuses industries sont soumises à des lois strictes (RGPD, HIPAA, etc.) qui imposent des normes élevées pour la sécurité des données.
- Préservation de la continuité des activités : Une attaque ou une faille dans le cloud peut interrompre les opérations, impactant la productivité et les revenus.

- Contrôle des accès et des mouvements de données.

1-5 Les types de service dans le cloud

L'évolution des modèles de service cloud sont proposés par des fournisseurs tiers sous forme de modules, et utilisés pour créer l'environnement dans le Cloud. Selon le type de service, vous pouvez gérer un degré différent des composantes du service [1] :

- **Le cœur de tout service tiers dans le Cloud** implique que le fournisseur gère le réseau physique, le stockage des données, les serveurs de données et les structures de virtualisation des ordinateurs. Le service est stocké sur les serveurs du fournisseur et virtualisé via son réseau géré en interne avant d'être livré aux clients et d'être accessible à distance. Cette solution permet de réduire les coûts de matériel et d'autres infrastructures afin de permettre aux clients d'accéder à leurs besoins informatiques de n'importe quel endroit au moyen d'une connexion Internet.

- Les services dans le Cloud en tant que **solution SaaS (logiciel en tant que service)** permettent aux clients d'accéder à des applications qui sont purement hébergées et exécutées sur les serveurs du fournisseur. Les fournisseurs gèrent les applications, les données, le temps d'exécution, les logiciels médiateurs ainsi que le système d'exploitation. La seule tâche des clients est de se procurer leurs applications. *Parmi les solutions SaaS, on peut citer Google Drive, Slack, Salesforce, Microsoft 365, Cisco WebEx et Evernote.*

- Les services dans le Cloud en tant que **solution PaaS (plateforme en tant que service)** offrent aux clients un hôte pour le développement de leurs propres applications, et celles-ci sont exécutées dans l'espace « bac à sable » du client sur les serveurs du fournisseur. Les fournisseurs gèrent le temps d'exécution, les logiciels médiateurs ainsi que le système d'exploitation. Les clients sont responsables de la gestion de leurs applications, de leurs données, de l'accès des utilisateurs, des appareils des utilisateurs finaux ainsi que des réseaux d'utilisateurs finaux. *Parmi les solutions PaaS, on peut citer Google App Engine et Windows Azure.*

- Les services dans le Cloud en tant que **solution IaaS (infrastructure en tant que service)** offrent aux clients le matériel et les structures de connectivité à distance nécessaires pour héberger l'essentiel de leur environnement informatique, jusqu'au système d'exploitation. Les fournisseurs ne gèrent que les services de base dans le Cloud. Les clients sont responsables de la sécurité de l'ensemble du système d'exploitation, y compris les applications, les données, les temps d'exécution, les logiciels médiateurs et le système d'exploitation lui-même. En outre, les clients doivent gérer l'accès des utilisateurs, les appareils administrés par les utilisateurs finaux ainsi que les réseaux d'utilisateurs finaux. *Parmi les solutions IaaS, on peut citer Microsoft Azure, Google Compute Engine (GCE) et Amazon Web Services (AWS).*

1-4 Les environnements dans le Cloud

Ils sont des modèles de déploiement dans lesquels un ou plusieurs services dans le Cloud créent un système pour les utilisateurs finaux et les organisations. Ces derniers répartissent les responsabilités de gestion (y compris la sécurité) entre les clients et les fournisseurs.

Les environnements dans le Cloud actuellement disponibles sont les suivants :

- **Les environnements publics dans le Cloud** sont composés de services dans le Cloud multi-locataires dans lesquels un client partage les serveurs d'un fournisseur avec d'autres clients, comme un immeuble de bureaux ou un espace de travail commun. Il s'agit de services tiers gérés par le fournisseur pour donner aux clients un accès via le Web.

- **Les environnements privés dans le Cloud fournis par des tiers** sont basés sur l'utilisation d'un service dans le Cloud qui offre au client l'utilisation exclusive de son propre Cloud. Ces environnements à locataire unique sont généralement détenus, gérés et exploités hors site par un prestataire externe.

- **Les environnements privés internes dans le Cloud** sont également composés de serveurs de services dans le Cloud à locataire unique, mais sont exploités à partir de leur propre centre de données privé. Dans ce cas, ces environnements dans le Cloud sont gérés par les entreprises elles-mêmes afin d'autoriser une configuration et un paramétrage complets de chaque élément.

- **Les environnements multi-cloud** comprennent l'utilisation de deux ou plusieurs services dans le Cloud provenant de fournisseurs distincts. Il peut s'agir de n'importe quelle combinaison de services publics ou privés dans le Cloud.

- **Les environnements hybrides dans le Cloud** comprennent une combinaison d'un centre de données privé dans le Cloud fourni par des tiers et/ou d'un centre de données privé dans le Cloud déployé sur site avec une ou plusieurs solutions publiques dans le Cloud.

2- FONCTIONNEMENT DE LA SÉCURITÉ DANS LE CLOUD

L'ensemble de mesure de sécurité proposer dans le cloud permet la récupération des données en cas de perte de données, Protéger le stockage et les réseaux contre le vol malveillant de données, d'empêcher les erreurs humaines ou les négligences qui sont à l'origine de fuites de données et de Réduire les conséquences de toute compromission des données ou du système.

La sécurité dans le cloud est structure autour de plusieurs piliers essentiels tels que [3] :

La sécurité des données est un aspect de la sécurité dans le Cloud qui comprend l'aspect technique de la prévention des menaces. Les outils et les technologies permettent aux fournisseurs et aux clients d'insérer des obstacles entre l'accès et la visibilité des données sensibles. Parmi ceux-ci, le *chiffrement* est l'un des plus puissants outils disponibles. Le chiffrement brouille vos données afin qu'elles ne soient lisibles que par une personne qui détient la clé de chiffrement.

La gestion des identités et des accès (IAM) concerne les privilèges d'accessibilité offerts aux comptes d'utilisateurs. La gestion de l'authentification et de l'autorisation des comptes d'utilisateurs s'applique également ici. *Les contrôles d'accès* sont essentiels pour empêcher les utilisateurs, tant légitimes que malveillants, d'entrer et de compromettre des données et des systèmes sensibles. La gestion des mots de passe, l'authentification à plusieurs facteurs et d'autres méthodes entrent dans le champ d'application de la gestion des identités et des accès.

La gouvernance se concentre sur les politiques de prévention, de détection et d'atténuation des menaces. Pour les PME et les grandes entreprises, des aspects tels que les *renseignements sur les menaces* peuvent contribuer au suivi et à la hiérarchisation des menaces afin de garder les systèmes essentiels bien protégés. Cependant, même les clients individuels de l'informatique dématérialisée pourraient tirer profit de la valorisation *des politiques et des formations relatives au comportement sûr des utilisateurs*. Ces règles s'appliquent principalement dans les environnements organisationnels, mais les règles de sécurité et de réaction aux menaces peuvent se révéler utiles à tout utilisateur.

La planification de la conservation des données (DR) et de la continuité des activités (BC) implique des mesures techniques de redressement après un incident en cas de perte de données. Au centre de tout plan de conservation des données et de continuité des activités se trouvent des méthodes de *redondance des données*, comme les sauvegardes. En outre, il peut être utile de disposer de systèmes techniques permettant d'assurer un fonctionnement ininterrompu.

La conformité juridique s'articule autour de la protection de la vie privée des utilisateurs, conformément aux dispositions des corps législatifs. Ainsi, les organisations doivent se conformer à des réglementations pour satisfaire à ces politiques. L'une des approches consiste à utiliser le *masquage des données*, qui permet de dissimuler l'identité à l'intérieur des données par des méthodes de chiffrement.

3- RISQUES LIÉS À LA SÉCURITÉ INFORMATIQUE DANS LE CLOUD

La sécurité dans le cloud rencontre plusieurs risques liés à une faible sécurité de ses services ceci pouvant entrainer une exposition des utilisateurs et des fournisseurs a toutes sortes de cybermenaces. Parmi ces menaces, nous pouvons citer [5]:

- Les risques liés à l'infrastructure du Cloud, y compris l'incompatibilité des structures informatiques existantes et l'interruption des services de stockage de données de tiers.
- Les menaces internes imputables à l'erreur humaine, comme une mauvaise configuration des contrôles d'accès des utilisateurs.
- Les menaces externes causées presque exclusivement par des acteurs malveillants, comme les logiciels malveillants, le phishing et les attaques DDoS.

Le principale risque lié à la sécurité du cloud est l'absence de périmètre de sécurité clairement défini. Contrairement aux approches traditionnelles de cybersécurité qui protégeaient le réseau, Les environnements cloud sont hautement interconnectes ce qui les exposent à des vulnérabilités tels que les API non sécurisées et améliorant le risque de détournement de comptes.

La dépendance a des fournisseurs tiers peut entrainer des pertes d'accès en cas d'interruption de service, comme des pannes de réseau ou de courant pouvant causer des pertes de données. Ces risques démontrent l'importance de disposer de sauvegardes locales pour les données critiques et d'adopter une approche de sécurité centrale sur le cloud en mettant une gestion rigoureuse des identités.

4- COMMENT SÉCURISER LE CLOUD ?

Plusieurs méthodes sont utilisées pour protéger les données dans le cloud. Parmi ces méthodes, nous avons :

Le **chiffrement** est l'un des meilleurs moyens de sécuriser vos systèmes informatiques dans le Cloud. Il existe plusieurs façons différentes d'utiliser le chiffrement, et elles peuvent être proposées par un fournisseur de services dans le Cloud ou par un fournisseur distinct de solutions de sécurité dans le Cloud[6] :

- Le **chiffrement des communications** avec le Cloud dans leur intégralité.
- **Le chiffrement de données particulièrement sensibles,** comme les identifiants de compte.
- Le **chiffrement de bout en bout** de l'ensemble des données qui sont chargées dans le Cloud.

Dans le Cloud, les données risquent davantage d'être interceptées lorsqu'elles sont en circulation. Lorsque vos données se déplacent d'un lieu de stockage à un autre ou lorsqu'elles sont transmises à votre application sur site, elles sont vulnérables. Par conséquent, le chiffrement de bout en bout est la meilleure solution de sécurité dans le Cloud pour les données importantes. Grâce au chiffrement de bout en bout, votre communication n'est à aucun moment accessible aux personnes extérieures sans votre clé de chiffrement.

Si vous utilisez le chiffrement, n'oubliez pas qu'il est primordial de gérer vos clés de chiffrement de manière sûre et sécurisée. Conservez une clé de sauvegarde et, dans l'idéal, ne la gardez pas dans le Cloud. Vous pouvez également envisager de modifier régulièrement vos clés de chiffrement de manière que toute personne qui y accède soit exclue du système au moment de la modification.

La **configuration** est une autre pratique efficace en matière de sécurité dans le Cloud. De nombreuses atteintes à la protection des données dans le Cloud sont dues à des vulnérabilités de base, comme des erreurs de configuration.

Voici quelques principes que vous pouvez suivre pour configurer:

1. **Ne laissez jamais les paramètres par défaut dans leur état d'origine**. L'utilisation des paramètres par défaut équivaut à ouvrir la porte d'entrée à un pirate informatique.
2. **Ne laissez jamais un bucket de stockage dans le Cloud ouvert.** Un bucket de stockage ouvert pourrait permettre aux pirates de voir le contenu simplement en ouvrant l'URL du bucket de stockage.
3. **Si le fournisseur de services dans le Cloud vous propose des commandes de sécurité que vous pouvez activer**, utilisez-les.

   Toute mise en œuvre du Cloud devrait également comporter des **conseils de base en matière de cybersécurité**. Même si vous utilisez le Cloud, il convient de tenir compte des pratiques standards de cybersécurité tels que:

- **Utilisez des mots de passe forts.** Utilisez un mélange de lettres, de chiffres et de caractères spéciaux pour rendre votre mot de passe plus difficile à pirater.
- **Utilisez un gestionnaire de mots de passe.** Vous pourrez attribuer des mots de passe distincts à chaque application, base de données et service que vous utilisez, sans avoir à les mémoriser tous.
- **Protégez tous les appareils** que vous utilisez pour accéder à vos données dans le Cloud, y compris les smartphones et les tablettes.
- **Sauvegardez régulièrement vos données** de manière que vous puissiez les restaurer intégralement en cas de panne du Cloud ou de perte de données chez votre fournisseur de services dans le Cloud
- **Modifiez les autorisations** pour empêcher toute personne ou tout appareil d'avoir accès à toutes vos données, sauf si cela s'avère nécessaire.
- **Protégez-vous avec des logiciels antivirus et antimalware**. Les pirates informatiques peuvent facilement accéder à votre compte si des logiciels malveillants s'introduisent dans votre système.
- **Évitez d'accéder à vos données sur un réseau Wi-Fi public**, surtout si celui-ci n'utilise aucune authentification solide. En revanche, utilisez un réseau privé virtuel (VPN) pour protéger votre passerelle vers le Cloud.

4. Le stockage dans le Cloud et le partage de fichiers

Les risques liés à la sécurité de l'informatique dans le Cloud peuvent avoir une incidence sur tout le monde, des entreprises aux consommateurs individuels.

N'oubliez pas que parmi ces services de stockage dans le Cloud généralement proposés, nombreux sont ceux qui ne chiffrent pas les données. Si vous souhaitez sécuriser vos données grâce au chiffrement, vous devrez utiliser un logiciel de chiffrement pour le faire vous-même avant de charger les données en ligne. Vous devrez alors remettre une clé à vos clients, faute de quoi ils ne pourront pas lire les fichiers.

5. Vérifier la sécurité de votre fournisseur de services dans le Cloud

La sécurité doit être l'un des principaux points à prendre en compte dans le choix d'un fournisseur de sécurité dans le Cloud. En effet, votre cybersécurité n'est plus seulement votre responsabilité : les entreprises de sécurité dans le Cloud doivent assumer leur part de responsabilité dans la création d'un environnement sécurisé dans le Cloud et assurer la sécurité des données.

Malheureusement, les entreprises proposant des services dans le Cloud ne vous dévoileront pas les principes fondamentaux de la sécurité de leur réseau. Cela équivaudrait à ce qu'une banque vous fournisse les détails de son coffre-fort ainsi que les numéros de combinaison de celui-ci.

Toutefois, si vous obtenez les bonnes réponses à certaines questions de base, vous pourrez être plus sûr que vos ressources dans le Cloud seront en sécurité. En outre, vous serez mieux à même de savoir si votre fournisseur a correctement traité les risques inhérents à la sécurité dans le Cloud. Nous vous recommandons de poser les questions suivantes à votre fournisseur de services dans le Cloud :

- **Audits de sécurité** : « Procédez-vous régulièrement à des audits externes de votre sécurité ? »
- **Segmentation des données** : « Les données relatives aux clients sont-elles segmentées logiquement et conservées séparément ? »
- **Chiffrement** : « Nos données sont-elles chiffrées ? Quelles sont les parties chiffrées ? »
- **Conservation des données des clients** : « Quelles sont les politiques appliquées en matière de conservation des données des clients ? »
- **Conservation des données des utilisateurs** : « Mes données sont-elles bien effacées si je quitte votre service dans le Cloud ? »
- **Gestion de l'accès** : « Comment les droits d'accès sont-ils contrôlés ? »

Assurez-vous également d'avoir lu les conditions d'utilisation (CGU) établies par votre fournisseur. La lecture des CGU est indispensable pour comprendre si vous recevez exactement ce que vous voulez et ce dont vous avez besoin.

5- SOLUTIONS

Plusieurs politiques et procédures peuvent être développer pour une utilisation plus sécuriser du cloud.

Nous précisons que les solutions varient en fonction des différentes utilisations du cloud (utilisation personnelle, pour petite et grandes entreprise…) [2].

5-1 Solutions hybrides de sécurité dans le Cloud

Les services hybrides de sécurité dans le Cloud peuvent être un choix très judicieux pour les PME et les grandes entreprises. Ils sont plus adaptés aux PME et aux grandes entreprises, car ils sont généralement trop complexes

pour un usage personnel. Cependant, ce sont ces organisations qui pourraient combiner l'évolutivité et l'accessibilité du Cloud tout en contrôlant sur place des données particulières.

Les avantages des systèmes hybrides de sécurité dans le Cloud sont :

La segmentation des services peut aider une organisation à contrôler la manière dont ses données sont consultées et stockées.

La redondance peut également être assurée grâce à des environnements hybrides dans le Cloud

5-2 Solutions de sécurité dans le Cloud pour les PME

Certaines entreprises peuvent recourir à un Cloud privé. Les particuliers et les petites entreprises doivent se contenter des services publics dans le Cloud. Par conséquent, votre sécurité doit être une priorité.

Dans les applications destinées aux petites et moyennes entreprises, vous constaterez que la sécurité dans le Cloud repose en grande partie sur les fournisseurs publics que vous utilisez.

Cependant, il existe des mesures que vous pouvez prendre pour assurer votre sécurité :

- **Segmentation des données multi-locataires** : les entreprises doivent s'assurer que leurs données ne sont accessibles à aucun autre client de leurs fournisseurs de services dans le Cloud.
- **Contrôles d'accès des utilisateurs** : le fait de contrôler les autorisations peut avoir pour effet de limiter l'accès des utilisateurs dans une mesure peu pratique.
- **Mise en conformité des données avec la législation** : il est essentiel que vos données soient conformes aux réglementations internationales, comme celles du RGPD, pour éviter de lourdes amendes et des atteintes à la réputation.
- **Mise à l'échelle rigoureuse des systèmes dans le Cloud** : avec la mise en œuvre rapide des systèmes dans le Cloud, assurez-vous de prendre le temps de vérifier la sécurité des systèmes de votre organisation par rapport au côté pratique.

5-3 Solutions de sécurité dans le Cloud pour les grandes entreprises

Plus de 90 % des grandes entreprises utilise le cloud. La sécurité du Cloud est un élément essentiel de la cybersécurité des entreprises. Les services privés dans le Cloud et d'autres infrastructures plus coûteuses peuvent être des solutions intéressantes pour les grandes entreprises. Cependant, vous devrez toujours vous assurer que le système informatique interne est en mesure d'assurer la maintenance de l'ensemble de vos réseaux.

Pour les grandes entreprises, la sécurité dans le Cloud peut se révéler bien plus flexible à condition d'investir dans votre infrastructure.

Il convient de garder à l'esprit quelques points clés :

- **Gérez activement vos comptes et vos services** : si vous n'utilisez plus un service ou un logiciel, fermez-le correctement.
- **Authentification à plusieurs facteurs (MFA)** : il peut s'agir de données biométriques, comme des empreintes digitales, ou d'un mot de passe et d'un code séparé envoyés à votre appareil mobile
- **Évaluez le rapport coût-bénéfice d'une solution hybride dans le Cloud** : la segmentation de vos données est bien plus importante dans le cadre d'une utilisation en entreprise, car vous traiterez des quantités de données beaucoup plus importantes.
- **Faites attention au Shadow IT** : il est essentiel de sensibiliser vos employés afin qu'ils évitent d'utiliser des services dans le Cloud non autorisés sur vos réseaux ou dans le cadre de leur travail au sein de votre entreprise.

  Ainsi, que vous soyez un particulier, une PME ou même une grande entreprise, il est important de veiller à ce que votre réseau et vos appareils soient aussi sécurisés que possible.

CONCLUSION

La sécurité dans le Cloud est une discipline de la cybersécurité dédiée à la sécurisation des systèmes informatiques dans le Cloud. Elle vise notamment à préserver la confidentialité et la sécurité des données dans les infrastructures, les applications et les plateformes en ligne. Pour sécuriser ces systèmes, il faut que les fournisseurs de services dans le Cloud et les clients qui utilisent ceux-ci consentent des efforts, qu'il s'agisse de particuliers, ou de petites, moyennes ou grandes entreprises.

Les fournisseurs de services dans le Cloud hébergent des services sur leurs serveurs grâce à des connexions Internet permanentes. Comme leur activité repose sur la confiance des clients, des méthodes de sécurité dans le Cloud sont utilisées pour préserver la confidentialité des données des clients et les stocker en toute sécurité. Aujourd'hui, la sécurité du cloud est une composante stratégique, avec des efforts constants pour anticiper les menaces. Cependant, la sécurité dans le Cloud reste aussi partiellement entre les mains du client. Il est essentiel de comprendre ces deux facettes pour trouver une solution saine de sécurité dans Cloud.

Références :

[1]HTTPS://WWW.HIVENET.COM/FR/POST/CLOUD-COMPUTING-HISTORY#:~:TEXT=LE%20CLOUD%20COMPUTING%20EST%20N%C3%A9,VERS%20DES%20SERVICES%20CLOUD%20MODERNES

[2]https://www.kaspersky.fr/resource-center/definitions/what-is-cloud-security

[3]- https://www.ibm.com/fr-fr/topics/cloud-security

[4]-https://www.hivenet.com/fr/post/cloud-computing-history#:~:text=LE%20CLOUD%20COMPUTING%20EST%20N%C3%A9,VERS%20DES%20SERVICES%20CLOUD%20MODERNES

[5]- https://cloud.google.com/learn/what-is-cloud-security?hl=fr

[6]- https://www.microsoft.com/fr-ca/security/business/security-101/what-is-cloud-security

[7]-https://www.cyberhaven.com/product/data-loss prevention?utm_medium=cpc&utm_source=google&utm_term=cloud%20data%20protection&utm_campaign=Unbranded&hsa_acc=9636236603&hsa_cam=21825303482&hsa_grp=169547844616&hsa_ad=718304646856&hsa_src=g&hsa_tgt=kwd-14478356985&hsa_kw=cloud%20data%20protection&hsa_mt=e&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=CjwKCAiA6aW6BhBqEiwA6KzDc4QylsaVHfZ6A4qofHGanQkIAsgCmyytTBdV0Jek7X5yI5J18OR3jBoCdqIQAvD_BwE

[8]-https://www.deepinstinct.com/dsx/dsx-cloud storage?_bt=690302844391&_bk=cloud%20data%20security&_bm=e&_bn=g&_bg=158063907349&utm_adgroup=158063907349&utm_gclid=CjwKCAiA6aW6BhBqEiwA6KzDc9hEQnElGj6P-AKnzJ8sVnR0Ugx9oRCed8CtCVGBWc7k63ovtD9ekRoCjggQAvD_BwE&utm_term=cloud%20data%20security&utm_campaign=kd-search-ww-storage-exact-20240207&utm_source=adwords&utm_medium=cpc&utm_content=690302844391&hsa_acc=8733123917&hsa_cam=20996028364&hsa_grp=158063907349&hsa_ad=690302844391&hsa_src=g&hsa_tgt=kwd-12613751656&hsa_kw=cloud%20data%20security&hsa_mt=e&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=CjwKCAiA6aW6BhBqEiwA6KzDc9hEQnElGj6P-AKnzJ8sVnR0Ugx9oRCed8CtCVGBWc7k63ovtD9ekRoCjggQAvD_BwE