Justification du champ d'étude

Introduction

Le travail à faire dans cette partie est de présenter la démarche que l'on adoptera afin de répondre aux besoins d'information. L'étude d'une technologie nécessite une justification et la délimitation du champ d'étude pour mieux cerner le sujet. Ensuite nous allons parler des techniques d'investigation et la revue documentaire pour effectuer cette étude.

Pour terminer nous allons parler de la sécurité informatique de manier globale.

La délimitation du champ d'étude correspond à une double délimitation. Il s'agit en effet de présenter la Blockchain as a Service dans sa globalité et l'application de ce dernier dans le secteur pharmaceutique.

II.2 Délimitation du champ de l'étude

Après avoir cadré l'étude, il est important de la délimiter. L'étude se fera sur la technologie blockchain. Mais plus spécifiquement, nous nous intéresserons au fonctionnement, la sécurité et le cas d'utilisation de la technologie blockchain. En effet, l'immensité des champs d'exploitation de la blockchain nous pousse à focaliser notre étude sur le secteur pharmaceutique.

II.3 Techniques d'investigation et revue documentaire

Pour satisfaire notre besoin d'informations et dans le but de répondre à la problématique posée plus haut nous avons eu recours aux différentes techniques suivantes :

- La recherche documentaire à travers Internet, les livres et études traitant du thème. Cette recherche a permis d'acquérir des connaissances sur les outils d'analyse d'obtenir des informations sur la blockchain et la BaaS.
- Une enquête a été menée dans le but de recueillir des données chiffrées concernant l'exploitation du réseau. Pour ce faire, nous avons usé des différents supports d'enquête, l'entretien et l'observation participante.

- Des entretiens avec les responsables du réseau ont favorisé le recueil d'information relatif à l'entreprise et à son activité.
- Enfin, l'observation a permis une meilleure compréhension et imprégnation du milieu blockchain, de ses acteurs et services.

II.4 La sécurité informatique

FIGURE 1 : LA SECURITE INFORMATIQUE

II.4.1 Définition

La sécurité informatique est un terme générique qui s'applique aux réseaux, à Internet, aux points de terminaison, aux API, au cloud, aux applications, à la sécurité des conteneurs et autres. Elle consiste à établir un ensemble de stratégies de sécurité qui fonctionnent conjointement pour vous aider à protéger vos données numériques. La sécurité informatique protège l'intégrité des technologies de l'information comme les systèmes, les réseaux et les données informatiques contre les attaques, les dommages ou les accès non autorisés.

La sécurité informatique consiste à protéger un système informatique contre toute violation, intrusion, dégradation ou vol de données au sein du système d'information.

La sécurité continue repose sur un système régulier de feedback et d'adaptation qui est généralement géré au moyen de points de contrôle automatisés. Grâce à l'automatisation, le feedback est rapide et efficace. Il ne ralentit pas le cycle de vie du produit. Cette méthode d'intégration de la sécurité vous permet de mettre en œuvre les mises à jour et les réponses aux incidents rapidement et globalement dans un environnement en constante évolution.

Avec l'essor d'internet, et l'utilisation par la majorité des entreprises et des organisations de processus informatisés, les menaces visant les systèmes d'informations n'ont cessés d'augmenter et de se sophistiquer, faisant aujourd'hui de la sécurité informatique une nécessité pour tous les types de structure.

La sécurité informatique vise généralement cinq principaux objectifs :

- **L'intégrité** : vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication
- **La confidentialité** : consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.
- **La disponibilité** : permettant de maintenir le bon fonctionnement du système d'information ;
- **La non répudiation** : permettant de garantir qu'une transaction ne peut être niée ;
- **L'authentification** : consistant à assurer que seules les personnes autorisées aient accès aux ressources.

Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

Quelle prestation de sécurité informatique choisir ?

II.4.2 Sécurité informatique : actions préventives

Les actions préventives sont les premières actions à mettre en œuvre pour assurer la sécurité informatique de son entreprise. Elles permettent de réduire le nombre de failles, d'intrusions, de tentatives de piratages et de pertes de données.

Parmi les actions préventives, on peut distinguer :

- La sensibilisation des utilisateurs :

L'humain étant le principal facteur de risque de sécurité au sein de votre système d'information, la sensibilisation des collaborateurs est primordiale.

Cette sensibilisation peut être effectuée par la mise en place d'une politique de sécurité informatique au sein de l'entreprise, d'une charte de sécurité informatique, de formations ou d'actions de sensibilisation.

- La mise en place d'outils de protection :
- Nous devons utiliser des outils de protections puissants, efficaces et abordables pour paliers aux problèmes de sécurité informatique les plus fréquents :
- Pare-feu de nouvelle génération pour protéger votre système d'information des intrusions.
- Antivirus professionnel pour protéger vos données des virus et repérer les logiciels malveillants.
- Solution antispam pour protéger votre messagerie des spams, phishing et messages malveillants.
- Avoir un système d'information performant, à jour et sécurisé :
  Maîtriser son système d'information et le tenir à jour est également une condition sine qua non d'une bonne protection informatique.
- L'audit de sécurité informatique :
  Pour mettre en place une politique de sécurité informatique adaptée, connaître son système d'information, la criticité de ses données, ses capacités de réaction en cas de problème, ou les moyens de protections les plus efficaces pour l'entreprise est indispensable.
  La réalisation d'un audit de sécurité permet à l'entreprise de prendre les meilleures décisions et de piloter sa stratégie efficacement.
- Mieux maîtriser la messagerie électronique avec une messagerie hébergée :

La messagerie électronique est l'un des modes de contamination des systèmes d'information les plus utilisés.

La mise en place d'une messagerie hébergée vous permet de vous assurer une gestion déléguée par nos équipes spécialisées en sécurité, des mises à jour continues et transparentes pour les utilisateurs et le recours à des antivirus, antipub et antispam intégrés.

II.4.2 Sécurité informatique : actions curatives

En cas d'incident, d'intrusion ou de contamination des postes ou des données, l'entreprise doit être prête à répondre à une situation d'urgence et à y faire face.

- PCA (Plan de Continuité d'Activité) / PRA (Plan de retour à l'activité)

Lorsqu'un incident de sécurité informatique intervient, il est nécessaire pour l'entreprise d'effectuer les procédures adaptées à la préservation des données ou des postes sains, à la conservation des preuves numériques, et à la continuité de l'activité ou à sa reprise dans des délais acceptable pour l'entreprise.

- Nettoyage des infections et remise en état de fonctionnement du système d'information

Après détection et enquête concernant la source et la nature de l'infection, nos équipes procèdent à un nettoyage de la contamination et, dans la mesure du possible, à une restitution de vos données et de l'intégrité de votre système d'information.

- Sauvegarde hébergée et redondante

Une sauvegarde externalisée, hébergée sur des serveurs hautement sécurisés et redondés, est la meilleure façon de préserver une copie de vos données, dans toutes les circonstances.

II.4.3 Mise en place d'une politique de sécurité

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification

et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.

Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les étapes suivantes :

- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

La politique de sécurité est donc l'ensemble des orientations suivies par une organisation en termes de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

A cet égard, il ne revient pas aux seuls administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers. Le rôle de l'administrateur informatique est donc de s'assurer que les ressources informatiques et les droits d'accès à celles-ci sont en cohérence avec la politique de sécurité définie par l'organisation.

De plus, étant donné qu'il est le seul à connaître parfaitement le système, il lui revient de faire remonter les informations concernant la sécurité à sa direction, éventuellement de conseiller les décideurs sur les stratégies à mettre en œuvre, ainsi que d'être le point d'entrée concernant la communication à destination des utilisateurs sur les problèmes et recommandations en termes de sécurité.

La sécurité informatique de l'entreprise repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation auprès des utilisateurs, mais elle doit aller au-delà et notamment couvrir les champs suivants :

- Un dispositif de sécurité physique et logique, adapté aux besoins de l'entreprise et aux usages des utilisateurs ;
- Une procédure de management des mises à jour ;
- Une stratégie de sauvegarde correctement planifiée ;
- Un plan de reprise après incident ;
- Un système documenté à jour ;

Conclusion

A la suite de la présentation du cadre d'étude, nous allons aborder la sécurité dans sa globalité. Ainsi dans la prochaine partie nous allons expliquer la blockchain, les cas d'utilisation, les BaaS et pour terminer la sécurité de la blockchain.