EPIGRAPHE

La folie c'est de faire toujours la même chose et s'attendre à un résultat différent

Albert Einstein

DEDICACE

A toute la famille NTAMBWE pour leurs soutient financièrement, physiquement et spirituellement

REMERCIEMENT

Ce travail qui sanction la fin de notre premier cycle à la faculté d'informatique, nous tenons à exprimer notre profonde gratitude et sincère remerciement à toute personne qui nous a appris en charge dès notre première année jusqu'à la réalisation de ce travail.

Je remercie le tout puissant de m'avoir donné la vie et la bonne santé et d'avoir fait de moi l'homme que je suis aujourd'hui.

Mon profond remerciement s'adresse à monsieur, Chef de travaux BONOMIE BOPE Co-directeur de ce travail pour ses sages conseils et orientation objectifs et qui nous a suivis le long de ce travail en dépit de ses périples occupations, sans oublier L'Assistant NZINGA DADY et mon chef DAN SENTRI et MIKE NSHIMPU, pour leurs grandes contributions dans l'élaboration de ce travail.

Nos remercîments le plus sincères vont à l'endroit de mes proches : mon père Samy NTAMBWE et ma mère Arlette NTUMBA ainsi qu'à mon frère beni NTAMBWE et mes sœurs grâce NTAMBWE, keren NTAMBWE, winner NTAMBWE et lajoie NTAMBWE

Sans toutefois oublier mes amies et collègue avec qui nous avons partagé ces cinq dernières années : chris MOTA, beni NZUNZI, apo MANANGA, grace LIWIKIA, jess YANGU, bryan ESCOBAR, kevin NDUKU, alex LUMANDE, serge PRECIEUX, exauce NGWEYI, henock BIGEKO et hodavia MASIAMINA

LISTE DES ABREVIATION

- **SQL :** Structured Query Language
- **AAA:** Authorization Authentication Accounting
- **ABIDS**:Application Based Intrusion Detection System
- **ACK :** Acknowledged, un accuse de réception
- **ACL:** Access Control List
- **AES:** Application Environment Services
- **ALCASAR :** Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié Réseau
- **API :** Application Programming Interface
- **C.A.F.E I&T :** Centre d'Assistance de Formation et d'Etude en Informatique et Télécommunications
- **CPU :** Central Processing Unit
- **DES :** Data Encryption Standard
- **DHCP:** Dynamic Host Configuration Protocol
- **DMZ :** DeMilitarized Zone
- **DoS:** Denis of Service
- **EAP-MD5:** Extensible Authentication Protocol- Message Digest 5
- **EAP-TLS**: Extensible Authentication Protocol - Transport Layer Security
- **ECC**: Error-Correcting Code
- **FAI :** Fournisseur d'Accès Internet
- **FTP:** File Transfer Protocol
- **GPL**: General Public License
- **HDD**: Hard Disk Drive
- **HIDS**: Host-based Intrusion Detection System
- **HIPS**: Host-based Intrusion Prevention System
- **HTTP**: HypertText Transfer Protocol
- **ICANN**: Internet Corporation for Assigned Names and Numbers
- **ICMP:** Internet Control Message Protocol
- **IDEA**: International Data Encryption Algorithm
- **IDS**: Intrusion Detection System
- **IETF**: Internet Engineering Task Force
- **INTERNIC**: INTERnet Network Information Center
- **IP:** Internet Protocol
- **IPNG**: Internet Protocol New Generation
- **IPS:** Intrusion Protection System
- **IPsec**: Internet Protocol SECurity
- **KIPS**: Kernel Intrusion Prevention System

- **L2FP**: Layer 2 Forwarding Protocol
- **L2TP:** Layer 2 Tunneling Protocol
- **LAN**: Local Area Network
- **LDAP**:Lightweight Directory Access Protocol
- **LMD**: Licence Master Doctorat
- **MAC**:Media Access Control
- **MIT**: Massachussetts Institute of Technology
- **NAC**: Network Access Control
- **NAP**: Network Access Point
- **NAT:** Network Address Translation
- **NIDS**:Network Intrusion Detection System
- **NIPS**: Network Intrusion Protection System
- **NNIDS:**Network Node Intrusion Detection system
- **NTIC :** Nouvelles Technologies de l'Information et de la Communication
- **OSI:** Open System Interconnection
- **PPTP**: Point to Point Tunneling Protocol
- **PSK** : Pre Shared Key
- **RADIUS**:Remote Authentication Dial-In User Service
- **RAM:** Random Access Memory
- **RFC:** Request For Comment
- **RPV:** Réseau Privé Virtuel
- **RSA :** Rivest Shamir Adleman
- **SNMP:** Simple Network Management Protocol
- **SPOF:** Single Point Of Failure
- **SSH:** Secure SHell
- **SSL**: Secure Socket Layer
- **SSO**: Single Sign-On
- **TCP/IP**: Transmission Control Protocol/Internet Protocol
- **UDP**: User Datagram Protocol

TABLE DE FIGURE

LISTE DE TABLEAU

1. INTRODUCTION GENERALE

La mise en place d'une mesure de sécurité contre les attaques informatiques est cruciale pour protéger un système informatique, contre les attaques nécessitant une approche systématique et proactive. En combinant des aspects techniques, organisationnels et humains, vous pouvez créer un environnement de sécurité robuste qui protège efficacement vos actifs informationnels.

De nos jours, la sécurité informatique est un défi crucial pour les entreprises et tous les acteurs qui l'entourent. Elle ne se limite plus à la fonction de l'informaticien. Il vise à préserver la confiance des utilisateurs et des clients à long terme. À moyen terme, l'objectif est de maintenir la cohérence de l'ensemble du système d'information, l'objectif est que chacun ait accès aux informations dont il a besoin de façon sûre et efficace.

La sécurité informatique est essentielle pour prévenir les attaques et les tentatives d'hameçonnage, le vol d'informations, les failles de sécurité et la destruction de biens. Tous les appareils tels que les tablettes et les smartphones sont de plus en plus menacés, car ils stockent désormais plus de données publiques et privées que la plupart des ordinateurs. En raison de l'augmentation exponentielle des cyberattaques l'année dernière, la plupart des entreprises et des particuliers subiront des interruptions de service et des vols de données.

Les entreprises sont souvent des cibles d'attaques par ransomware, qui obligent la victime à payer une rançon au pirate pour que celui-ci restaure les actifs de l'entreprise. Il est essentiel d'être préparé et de disposer des outils et des ressources requis pendant et après tout attaque.

La sécurité des réseaux consiste à prendre des mesures préventives pour protéger l'infrastructure réseau sous-jacente contre tout accès non autorisé, toute utilisation abusive, tout dysfonctionnement, toute modification, toute destruction ou toute divulgation inappropriée. La mise en œuvre de ces mesures permet aux ordinateurs, aux utilisateurs et aux programmes d'exécuter leurs fonctions critiques autorisées dans un environnement sécurisé. Certaines menaces visent à interrompre les activités d'une organisation et non pas à collecter silencieusement des informations en vue de gains financiers ou d'espionnage. L'approche la plus pratiquée est l'attaque par déni de service (DoS, Denial of Service). Ce type d'attaque submerge les ressources du réseau (par exemple les passerelles Web et de messagerie, les routeurs, les commutateurs, etc.), interdit l'accès aux utilisateurs et aux applications, puis finit par interrompre totalement le service ou par dégrader fortement sa qualité.

L'attaque n'exige pas nécessairement de travail de piratage actif de la part de ses auteurs, mais dépend plutôt de leur capacité à multiplier le trafic vers l'organisation pour profiter d'une infrastructure mal configurée ou médiocrement protégée. Le plus souvent, cela signifie qu'ils utilisent un réseau de systèmes informatiques compromis qui collaborent pour submerger la cible, une attaque dite par déni de service distribué (DDoS, Distributed Denial of Service).

2. PROBLEMATIQUE

La mise en place de mesures de sécurité contre les attaques informatiques est une tâche complexe qui nécessite une approche intégrée. Les organisations doivent évaluer soigneusement ces problématiques pour développer des stratégies de sécurité efficaces et durables, tout en maintenant une culture de sécurité au sein de l'entreprise. Dans cette

perspective les entreprises, dans le but d'échanger les informations, elles sont appelées à implémenter une mesure de sécurité pouvant bien sécuriser les informations pour reduire la vulnérabilité partant de ce qui précède, nous formulons les questions suivantes
Quel est la meilleure façon d'éviter les attaques réseau ?

3. HYPOTHESES

Une hypothèse est une supposition que l'on fait de certaines choses pour tirer des conséquences à vérifier. En répondant aux questions posées ci-haut nous émettons les hypothèses suivantes :

- Mettre à jour régulièrement les systèmes et applications.
- Former le personnel aux risques de sécurité.
- Effectuer des sauvegardes fréquentes des données importantes.
- Renforcer un moyen de pare-feu pour la sécurité des informations

4. CHOIX ET INTERET DU SUJET

Nous avons choisi ce sujet pour la simple raison qu'un constat a été remarqué selon lequel les institutions n'arrivent plus à bien sécuriser les informations. Cette étude permettra à l'occurrence aux dirigeants des institutions de bien appréhender et mettre en place les techniques de protection d'information dans leur réseau. Cela dit, nous allons présenter les différentes raisons qui nous ont poussés à réaliser ce travail et cela sur différents plans à l'occurrence :

- Sur le plan personnel : ce travail est non seulement une réalisation comme l'exige le ministère de l'enseignement supérieur et universitaire enfin d'obtenir un diplôme, mais aussi cette étude nous aidera à bien comprendre et maitriser la notion sur la sécurité informatique dans une entreprise publique ou privée.
- Sur le plan scientifique : ce travail est un couloir aux autres chercheurs qui se sentiront être capable d'accroitre ou améliorer leur performance en matière de la sécurité informatique
- Sur le plan social : Ce travail offre une solution de sécurité qui garantit à tous les utilisateurs de MENZIES une authentification sécurisée, évitant ainsi toute manipulation des données.

5. OBJECTIFS DU TRAVAIL

5.1 OBJECTIF GENERAL

Aux jours d'aujourd'hui, il est difficile dans une société d'évoluer sans avoir une protection des donnée et vu l'importance de ce dernier, les utilisateurs, les écoles, les universités, les entreprises cherchent de moyens pour arriver à satisfaire ce besoin qui s'avère indispensable dans la vie quotidien, d'où la création d'un système de sécurité. Cela étant dit, nous envisageons à la fin de ce travail montrer et faire comprendre aux dirigeants des entreprises de l'importance d'avoir un système de sécurité.

5.2 **OBJECTIFS SPECIFIQUES**

Dans le but de réaliser notre objectif général assigné à ce travail, nous nous sommes proposé les objectifs spécifiques suivants :

- Mise en place d'un système de sécurité contre les attaques.
- Expliquer tant soit peu l'importance de mise en place d'un système de sécurité contre les attaques.

5. DELIMITATION DU TRAVAIL

Dans ce point, nous allons présenter nos champs d'application. En tant qu'une œuvre scientifique, notre travail est délimité à la mise en place d'un système de sécurité contre les attaques et par rapport au temps

Par rapport au temps, nos investigations couvrent la période allant d'octobre 2024 à juillet 2025.

7. DIFFICULTES RENCONTREES

Sur le plan financier : les difficultés d'ordre financier ont handicapé quelques peu nos déplacements et nos opérations de photocopie sans mettre en doute la fiabilité des résultats de notre travail, ces difficultés ont sûrement empêché de scruter plus à fond certains éléments.

8. SUBDIVISION DU TRAVAIL

Notre travail est intitule « la Mise en place d'une mesure de securite contre les attaquer externe » hormis l'introduction et la conclusion, le present travail comporte Cinq chapitres :

Chap I GENERALITE SUR LA SECURITE INFORMATIQUE

Chap II NOTION SUR LES ATTAQUES

Chap III CADRAGE DU PROJET

Chap IV ETUDE DU SITE MENZIES

Chap V MISE EN ŒUVRE

Chap I **GENERALITE SUR LA SECURITE INFORMATIQUE**

I.1 **INTRODUCTION**

Comme des informations confidentielles circulent dans les réseaux, la sécurité des communications est devenue préoccupation importante des utilisateurs et des entreprises. Tous cherchent à se protéger contre une utilisation frauduleuse de leurs données ou contre des intrusions malveillantes dans les systèmes informatiques. Par ailleurs, une multitude de virus se propagent à l'insu des utilisateurs dans les fichiers télécharges. Les virus sont susceptibles de détruire des documents ou même de provoquer la perte totale des informations stockées dans les machines. La tendance actuelle est de mettre en place des mécanismes de contrôle d'accès et des protocoles sécurises qui apportent plusieurs services : l'authentification, la confidentialité, l'intégrité, disponibilité et non répudiation

I.2 **SECURITE INFORMATIQUE**

La sécurité informatique est un domaine crucial qui vise à protéger les systèmes, les réseaux et les données contre les attaques, les dommages et les accès non autorisés.

Dans une entreprise, le réseau a principalement pour but l'échange de ces ressources desquelles dépendent les activistes commerciales de l'entreprise. Etant donné que ces ressources sont cruciales à son bon fonctionnement, il est important, voire obligatoire, de veiller à leur sécurité.

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettent de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

Dans une entreprise, le réseau a principalement pour but l'échange de ces ressources desquelles dépendent les activistes commerciales de l'entreprise. Etant donné que ces ressources sont cruciales à son bon fonctionnement, il est important, voire obligatoire, de veiller à leur sécurité.

N.B : La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matériels ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

I.2.1 **OBJECTIF DE LA SECURITE INFORMATIQUE**

L'objectif de la sécurité informatiques d'assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu et par des personnes autorisées.

La sécurité informatique à plusieurs objectifs bien sur lie aux types de menaces ainsi qu'aux types de ressources, etc… néanmoins, les points principaux sont les suivants :

- Empêcher la divulgation non-autorisée de données ;
- Empêcher la modification non – autorisée de données ;

- Empêcher l'utilisation non autorisée de ressources réseau ou informatique de façon générale.

I.2.2 Définition sur le concept sécurité

- **Sécurité informatique**

La sécurité en informatique est un domaine crucial qui vise à protéger les systèmes informatiques, les réseaux et les données contre les attaques, les dommages ou les accès non autorisés.

- **Logiciels malveillants**

Les logiciels malveillants sont des logiciels qui ont été développés dans le but de nuire : collecte d'informations, hébergement d'informations illégales, etc. Afin de s'installer sur un ordinateur, certains logiciels malveillants exploitent les vulnérabilités du système d'exploitation ou des applications. Ils s'appuient sur des erreurs de conception ou de programmation pour détourner le déroulement des programmes à leur avantage.

- **Vulnérabilité**

Faiblesse / faille : faute accidentelle ou intentionnelle introduite dans spécification, conception ou configuration du système.

- **Attaque**

Action malveillante qui tente d'exploiter une faiblesse dans le système et de violer un ou plusieurs besoins de sécurité.

- **Intrusion**

Faute opérationnelle, externe, intentionnellement nuisible, résultant de l'exploitation d'une vulnérabilité dans le système

- **Bombe logique**

Partie de programme qui reste dormante dans le système hôte jusqu'à ce qu'un instant ou un événement survienne, ou que certaines conditions soient réunies, pour déclencher des effets dévastateurs en son sein.

- **Porte dérobée /backdoors**

Moyen de contourner les mécanismes de sécurité ; il s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle (cheval de Troie en particulier) Ces passages secrets sont ménagés par les concepteurs de logiciels pour fournir des accès privilégiés pour les tests ou la maintenance. Mais les pirates qui les découvrent peuvent déjouer tous les mécanismes de sécurité et rentrer dans le système.

- **Virus**

Segment de programme qui, lorsqu'il s'exécute, se reproduit en s'adjoignant à un autre programme (du système ou d'application), et qui devient ainsi un cheval de Troie ;

- **Spyware**

Contraction de spy et software. Logiciel espion qui collecte des données personnelles avant de les envoyer à un tiers ; Exemple : Keylogger : transmettre les données saisies au clavier.

- **Méthode classique**

Faire crouler le serveur sous une masse de requêtes généralement mal formées à dessein pour entraîner une réponse anormale et paralysante. L'attaque utilise très souvent une multitude de PC zombies travaillant de concert, infectés par des backdoors/chevaux de Troie et mobilisables à distance par un pirate. Il est aussi possible de bloquer à distance des routeurs en tirant parti de failles de leur software.

I.2.3 DEFINITION SUR LE CONCEPT CRYPTOGRAPHIE

De tout temps, les codes ont existé. Ils ont d'abord servi à retranscrire des idées, à écrire un langage. L'homme a perçu le besoin de cacher, de dissimuler des informations personnelles ou confidentielles, et cela bien avant l'ère informatique. Mais avec ces nouveaux moyens de communication est arrivée la nécessité de protéger le contenu de certains messages des inévitables curieux. Ainsi est apparue la cryptographie= la science ou l'art de dissimuler ou cacher des messages ou textes ou…etc (le rendre inutilisable…). Autrement dit, la science qui crée des cryptogrammes (à l'aide de codes secrets pour chiffrer et déchiffrer). Essentiellement, il y'a deux méthodes fondamentales pour la cryptographie classique pendant la seconde guerre mondiale : transposition, substitution.

- **Sténographie**

Contrairement à la cryptographie, qui chiffre des messages de manière à les rendre incompréhensibles, la sténographie (en grec « l'écriture couverte ») cache les messages dans un support, par exemple des images ou un texte qui semble anodin (comme l'alphabet bilitère de Francis Bacon ou les fameuses lettres de George Sand). L'idée est la même pour les grilles de Cardan et le « barn code » : on noie le message dans un autre et seuls certains mots doivent être lus pour découvrir le texte caché.

- **Cryptographie**

Discipline incluant les principes, les moyens et les méthodes de transformation des données, dans le but de masquer leur contenu, d'empêcher leur modification ou leur utilisation illégale.

- **La cryptologie**

Est l'étude des techniques de chiffrement et de déchiffrement des informations, ainsi que l'analyse des systèmes de communication sécurisés. Elle se divise principalement en deux branches : la cryptographie et la cryptanalyse.

- **Cryptographie**

Ensemble des techniques qui permettent de rendre un message inintelligible pour quiconque n'a pas la clé de déchiffrement. Elle vise à protéger la confidentialité, l'intégrité et l'authenticité des données.

- **Cryptanalyse**

Science qui consiste à déchiffrer des messages sans posséder la clé utilisée pour le chiffrement, souvent en exploitant des faiblesses dans les algorithmes ou les systèmes de chiffrement.

- **Chiffre**

Ensemble de procédés et ensemble de symboles (lettres, nombres, signes, etc.) employés pour remplacer les lettres du message à chiffrer. On distingue généralement les chiffres à transposition et ceux à substitution.

- **Décrypter**

Parvenir à restaurer des données qui avaient été chiffrées, donc à leur faire retrouver leur état premier ("en clair"), sans disposer des clefs théoriquement nécessaires.

- **Clef**

Dans un système de chiffrement, elle correspond à un nombre, un mot, une phrase, etc. qui permet, grâce à l'algorithme de chiffrement, de chiffrer ou de déchiffrer un message.

I.3. LE PRINCIPE DE LA SECURITE

La sécurité repose sur 3 principes fondamentaux, regroupé au sein de la triade : C.I.A (Confidentiality, Integrity and Availability ; en français : Confidentialité, Intégrité et Disponibilité).

I.3.1 LES PRINCIPES FONDAMENTAUX

- **La confidentialité**

La confidentialité est le fait de s'assurer qu'une information est accessible uniquement par les entités qui ont le droit d'accéder à celle-ci. Dans le cadre où nous avons à faire à des données sensibles (données de l'armée, gouvernementales etc…) ce principe est souvent respecté. Il est important de respecter ce principe, imaginez qu'un tiers arrive à obtenir la liste des cartes bancaires des clients d'une banque… Cela peut être extrêmement dommageable pour la banque ainsi que pour les clients.

- **L'intégrité**

L'intégrité s'assure que la donnée reste toujours intègre c'est-à-dire qu'elle n'a pas été modifiée par un tiers non autorisé. Ce principe devra être respecté tout au long de la vie de l'information. Garantir l'intégrité d'une donnée, c'est garantir que la donnée est restée fiable

depuis sa création. Prenons le cas où un hacker arrive à s'introduire sur les comptes bancaires des clients d'une grande banque et dérobe de l'argent, il y a alors altération de la donnée ainsi qu'un préjudice financier (plus ou moins important suivant l'importance de l'attaque) pour la banque.

- **La disponibilité**

La disponibilité est le fait de s'assurer que l'information soit toujours disponible peu importe le moment choisit.

I.3.2 LES PRINCIPES COMPLEMENTAIRES

L'Authenticité

Au sein d'un système d'information, il est important de vérifier l'authenticité de chaque ressource. Cela est possible grâce au mécanisme d'authentification, qui permet de prouver l'identité d'une personne via le processus d'identification. Une authentification est qualifiée de « forte » lorsqu'au moins deux contrôles interviennent dans le processus d'identification. Par exemple, une authentification forte serait de vérifier une identité avec un lecteur de carte à puce ainsi qu'avec un scanner biométrique.

- **L'anti-rejet**

L'anti-rejet fait généralement référence à des mécanismes et des techniques utilisés pour prévenir le rejet des modifications ou des mises à jour dans des systèmes ou des applications. Cela peut inclure la gestion des changements, la migration de données, et l'adoption de nouvelles technologies.

- **Non-répudiation**

La non-répudiation se base sur un principe simple : une entité ne peut nier son implication dans une action à laquelle il a participé. Ce principe peut être respecté via différent mécanismes : les signatures numériques, un système d'accounting (log des actions faites…). Le but de la non-répudiation est de contrôler chaque action fais sur un réseau afin de savoir quelle entité est à l'origine d'une action et/ou d'une défaillance sur le système d'information.

I.4 TYPOLOGIE DES RISQUES INFORMATIQUES

En sécurité informatique, il existe deux grands types des risques à savoir : les risques humains et les risques matériels.

I.4.1 **RISQUES HUMAINS**

Ce sont les plus importants, même s"ils sont le plus souvent ignorés ou minimisés. Ils concernent les utilisateurs mais également les informaticiens eux- mêmes.

On peut citer :

- **La maladresse**

Commettre des erreurs ou exécuter de traitement non souhaité, ou effacer involontairement des données ou des programmes; etc…

- **L'inconscience et l'ignorance**

Introduire des programmes malveillants sans le savoir (par exemple lors de la réception du courrier). Des nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils font courir aux systèmes qu'ils utilisent. Réaliser des manipulations inconsidérées (autant avec des logiciels qu'avec du matériel).

- **La malveillance**

Ces dernières années, il est impossible d'ignorer les différents problèmes de virus et des vers. Certains utilisateurs peuvent volontairement mettre en péril le système d'informations, en y introduisant en connaissance de cause de virus ou en introduisant volontairement des mauvaises informations dans une base des données. On parle même de la « cybercriminalité »

- **L'ingénierie sociale :**

Une méthode pour obtenir d'une personne des informations confidentielles, que l'on n'est pas normalement autorisé à obtenir, en vue de les exploiter à d'autres fins. Elle consiste à :

- Se faire passer pour quelqu'un que l'on n'est pas (en général un administrateur réseau)
- Demander des informations personnelles (nom de connexion, mot de passe, données confidentielles, etc.) en intervenant un quelconque prétexte (problème dans le réseau, modification de celui-ci, etc.) ; Elle peut se faire soit au moyen d'une simple communication téléphonique ; soit par mail, soit en se déplaçant directement sur place.

- **L'espionnage**

Surtout industriel, emploie les même moyens, ainsi que bien d'autres, pour obtenir des informations sur des activités concurrentes, procédés de fabrication, projets en cours, futurs produits, politique de prix, clients et prospects, etc…

I.4.2 RISQUES MATERIELS

Ils sont liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels. Ces incidents sont plus ou moins fréquents selon les soins apportés lors de la fabrication et de l'application des procédures de tests effectués avant que les ordinateurs et les programmes ne soient mis en service. Certaines de ces pannes ont des causes indirectes, voire très indirectes, donc difficiles à prévoir. On peut citer :

- **Les incidents liés au matériel**

La plupart des composants électroniques modernes produits en grandes séries, peuvent comporter des défauts de fabrication. Ils finissent un jour ou l'autre par tomber en panne. Certains de ces pannes sont assez difficiles à déceler car intermittentes ou rares. Parfois, elles relèvent d'une erreur de conception.

- **Les incidents liés au logiciel**

C'est sont les plus fréquents. Les systèmes d'exploitation et les programmes sont de plus en plus complexes car ils font de plus en plus de choses. Ils nécessitent l'effort conjoint de dizaines, de centaines, voire de milliers de développeurs.

- **Les incidents liés à l'environnement**

Les machines électroniques les réseaux de communication sont sensibles aux variations de températures ou d'humidité ainsi qu'aux champs électromagnétiques. Dès lors, il est possible qu'un ordinateur tombe en panne de manière définitive ou intermittente à cause des conditions climatiques inhabituelles ou par l'influence d'installations électriques notamment industrielles.

I.5 ETUDES DES RISQUES LIES A LA SECURITE INFORMATIQUE

Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi. Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés. L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque.

On obtient ainsi la liste de ce qui doit être protégé :

- câble arraché
- coupure secteur
- crash disque
- mauvais profil

En fait, avec le développement de l'utilisation d'internet, nombre d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, elles sont plus au niveau de l'architecture trois tiers ou n-tiers. Il devient donc nécessaire de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système. En revanche, la sécurité est un compromis entre coûts, risques et contraintes.

On comprendra mieux le poids d'un risque en se fiant à la formule suivante : **« *Risque* = Menace x Vulnerabilite/Contre mesure »**

- **Risque :** C'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit, c'est une possibilité qu'un fait dommageable se produise.
- **Vulnérabilité :** C'est une faiblesse inhérente à un système (software ou hardware). Appelée parfois faille ou brèche, elle représente le niveau d'exposition face à la menace dans un contexte particulier.
- **Menace :** C'est le danger (interne ou externe) tel qu'un hacker, un virus, etc.

- **Contre-mesure :** C'est un moyen permettant de réduire le risque dans une organisation.

I.5.1. **CONSEQUENCES DE LA FORMULE**

- Le risque est d'autant plus réduit que les contre-mesures sont nombreuses
- Le risque est plus important si les vulnérabilités sont nombreuses.

L'utilisation de l'outil informatique est susceptible de nous exposer à plusieurs types des risques. Il importe donc de pouvoir mesurer ces risques en fonction de la probabilité ou de la fréquence de leurs survenances et aussi en mesurant leurs effets possibles. Ces effets peuvent avoir des conséquences négligeables ou catastrophiques :

- Le traitement informatique en cours échoue : il suffit de le relancer, éventuellement par une autre méthode si on craint que la cause ne réapparaisse
- L'incident est bloquant et on doit procéder à une réparation ou une correction avant de poursuivre le travail entrepris. Il est cependant à noter que ces mêmes incidents peuvent avoir des conséquences beaucoup plus fâcheuses.
- Données irrémédiablement perdues ou altérées, ce qui les rend inexploitables par la suite…
- Données ou traitements durablement indisponibles, pouvant entrainer l'arrêt d'une production ou d'un service.
- Divulgation d'informations confidentielles ou erronées pouvant profiter à des sociétés concurrentes ou nuire à l'image de marque de l'entreprise
- Déclenchement d'actions pouvant provoquer des accidents physiques ou induire des humains.

I.6 **GESTION DES RISQUES INFORMATIQUES**

La gestion des risques informatiques est un ensemble d'opérations de gérer et de diriger les différentes incidences liées à la manipulation de l'outil informatique. La gestion des risques consiste en trois actions majeures :

- Etudier les risques potentiels (identifier/mettre au jour ces risques)
- Imposer des règles de sécurité adéquates pour réduire ces risques
- Formation des utilisateurs.

I.6.1 **ETUDIER LES RISQUES POTENTIELS**

Cette phase consiste à faire un examen intégral de la méthodologie de l'étude des risques informatique en vigueur. Cela se matérialise aux moyens

- **Définition de l'environnement**

Définition des acteurs et leurs intérêts ; Importance de la sécurité dans la stratégie de l'entreprise ; Type de données impliquées ; Visibilité extérieure de la sécurité (importance pour la clientèle, le public).

- **Etude des menaces**

Identifier la nature de la menace: accidentelles (désastre, bugs…) ou intentionnelles (attaques, vols…) ; S'enquérir des sources de la menace: personnel non autorisé, intrus, logiciel ; Localiser la menace : procédures manuelles, informatique (software, réseau, stockage, hardware), infrastructure (concrète et abstraite).

- **Estimation du risque et du plan stratégique**

Risque (Coût des pertes à court, moyen et long terme engendrées, Coût de la mise en place de la contre- mesure tant au niveau logique que logistique, Comparer la perte potentielle au coût de la contre-mesure) ; Plan stratégique (Planning de l'implémentation avec prise en compte des besoins futurs en termes de sécurité ou non, Planning du suivi de l'implémentation).

- **Mise en place du plan de sécurité**

Les mécanismes de sécurité mis en place peuvent gêner les utilisateurs et les consignes et règles y définies peuvent devenir 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. Raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité dont la mise en œuvre s'effectue en quatre phases:

- 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.

- **Audit de sécurité**

L'audit de sécurité consiste à s'appuyer sur un tiers de confiance (de préférence une société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre, au regard de la politique de sécurité. En fait, l'objectif de l'audit est ainsi de vérifier que chaque règle de la politique de sécurité est correctement appliquée et que l'ensemble des dispositions prises forme un tout cohérent.

I.6.2 **IMPOSER DES REGLES DE SECURITE ADEQUATES**

Ceci consiste en la définition de procédures internes à l'entreprise basées sur :

- **Des règles administratives** Suivre des standards de sécurité (normes ISO) ; Suivre les lois.
- **Des règles physiques** Gardent, caméras, alarmes, verrous et Accès aux locaux sécurisés par biométrie.
- **Des règles techniques** - Déterminer des niveaux de classification des données ; Définir des niveaux d'accès à ces données ; Utiliser la cryptographie pour le traitement et le stockage de l'information ; Mettre en place un firewall matériel et/ou logiciel, …

I.6.3 **FORMATION DES UTILISATEURS**

Il est de plus en plus admis que la sécurité est essentielle. Les coûts engendrés par les pertes de données dues aux attaques réseaux et autres malwares diminuent sensiblement d'années en années1. Il est beaucoup plus simple de corrompre l'utilisateur et ce qui l'entoure que l'algorithme de chiffrement utilisé comme par exemple :

- L'utilisateur ne connait pas les risques engendrés par la conservation de la liste des mots de passe utilisés à côté de l'ordinateur.
- Il est souvent plus simple de s'introduire dans l'ordinateur de l'utilisateur afin de retrouver le texte en clair (hacking, vol,….)
- Il est possible de l'espionner, le pousser à la délation, pratiquer le shouldersurfing ou tout autre technique dite de "social engineering", …

Il ne s'agira donc pas ici d'expliquer aux employés comment fonctionnent les algorithmes qu'ils utiliseront, mais plutôt comment et dans quelles conditions ils devront les utiliser en définissant des règles qui ne devront pas être transgressées. Il y a également plusieurs manières de réagir à un risque, des plus « sûres » aux plus inconscientes.

- Transférer les risques à une compagnie d'assurances
- Réduire les risques en implémentant des contre-mesures qui peuvent être
- Dissuasives : empêcher une attaque
- Préventives : faire échouer une attaque
- Correctrices : réduire les dommages causés par une attaque
- Ignorer/Négliger les risques
- Accepter les risques si les contre-mesures sont trop onéreuses

Certes, il y a toujours un risque, aussi infime soit-il. Il faudra donc peser le pour et le contre lors de la mise en place éventuelle d'une contre-mesure. Toutefois, en 2007.on remarque une remontée de la somme totale des pertes, due à la fraude financière.

I.7 **INSTALLATION ET COMPOSANTES D'UNE POLITIQUE DE SECURITE INFORMATIQUE**

L'élément de politique de sécurité est l'ensemble des orientations suivies par une organisation en termes de sécurité. Elle est élaborée au niveau de système de pilotage (Direction), car elle concerne tous les utilisateurs du système. 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 aussi aller au-delà de cela tout en couvrant les champs ci-après :

- Mise en place des correctifs
- Définition de la police de sécurité
- Objectifs, Portée, Responsables
- Une stratégie de sauvegarde correctement planifiée
- Description de la sécurité (de l'infrastructure physique, des données informatiques, des applications, du réseau)
- Plan en cas de sinistre (Un plan de reprise après incident)
- Sensibilisation du personnel aux nouvelles procédures

Il ne faut pas également perdre de vue que la sécurité est comme une chaîne, guère plus solide que son maillon le plus faible. En plus de la formation et de la sensibilisation permanente des utilisateurs, la politique de sécurité peut être découpée en plusieurs parties :

- **Défaillance matérielle**

Tout équipement physique est sujet à défaillance (usure, vieillissement, défaut…) ; L'achat d'équipements de qualité et standard accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction. Seule une forme de sauvegarde peut cependant protéger les données.

- **Défaillance logicielle**

Tout programme informatique contient des bugs. La seule façon de se protéger efficacement contre ceux-ci est de faire des copies de l'information à risque. Une mise à jour régulière des logiciels et la visite des sites consacrés à ce type de problèmes peuvent contribuer à en diminuer la fréquence.

- **Accidents (pannes, incendies, inondations…)**

Une sauvegarde est indispensable pour protéger efficacement les données contre ces problèmes. Cette procédure de sauvegarde peut combiner plusieurs moyens fonctionnant à des échelles de temps différentes : Disques RAID pour maintenir la disponibilité des serveurs ; Copie de sécurité via le réseau (quotidienne) ; Copie de sécurité dans un autre bâtiment (hebdomadaire).

- **Vol via des dispositifs physique (disques et bandes)**

Contrôler l'accès à ces équipements : ne mettre des unités de disquette, bandes… que sur les ordinateurs où c'est essentiel. Mettre en place des dispositifs de surveillances.

- **Piratage et virus réseau**

Cette problématique est plus complexe et l'omniprésence des réseaux, notamment l'Internet, lui confère une importance particulière. Les problèmes de sécurité de cette catégorie sont particulièrement dommageables et font l'objet de l'étude qui suit.

I.8 PRINCIPAUX DEFAUTS DE SECURITE INFORMATIQUE

Les défauts de sécurité peuvent être considérés comme des modifications accidentelles ou inconscientes du fonctionnement normal des équipements informatiques. Les défauts de sécurité d'un système d'information les plus souvent constatés sont :

Installation des logiciels et matériels par défaut.

- Mises à jour non effectuées.
- Mots de passe inexistants ou par défaut.
- Services inutiles conservés (Netbios…).
- Traces inexploitées.
- Pas de séparation des flux opérationnels des flux d'administration des systèmes.
- Procédures de sécurité obsolètes.
- Eléments et outils de test laissés en place dans les configurations en production.

Chap II **NOTION SUR LES ATTAQUES**

II.1 **INTRODUCTION**

Chaque ordinateur connecté à Internet et d'une manière plus générale à n'importe quel réseau informatique, est susceptible d'être victime d'une attaque d'un pirate informatique. Ainsi, il est nécessaire de se protéger de ces attaques réseaux en installant un dispositif de protection. Dans ce chapitre, nous verrons comment protéger les systèmes efficacement face à ces menaces. Mais avant cela, il est important, pour comprendre le rôle précis de ces systèmes, de faire un parle sur les menaces, les risques, les principales d'attaques et les moyens de protection du système informatique.

II.2. **DEFINITION DE CONCEPTS**

- Le système informatique : le système d'information représente l'ensemble des données de l'entreprise ainsi que ses infrastructures matérielles et logicielles. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger[1]
- Sécurité des réseaux informatiques : la sécurité des réseaux consiste à mettre en place des moyens en vue de garantir les propriétés de sécurité concernant des données critiques d'une entreprise, ainsi que de faire appliquer les règles définies dans une politique de sécurité [2]
- Sécurité informatique : c'est l'ensemble des moyens mis en œuvre pour Réduire la vulnérabilité d'un système contre les menaces accidentelles ou Intentionnelles.

II.3. **PRINCIPE DE LA SECURITE INFORMATIQUE**

La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaine en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

La sécurité informatique régis 5 principes :

[1] Jean-François pilou et Jean-Philippe Bay. Sécurité informatique .3ieme édition, Dunod, Paris 2013, P24
[2] Idem

- **La confidentialité :** Seule les personnes habilitées doivent avoir accès aux données. Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension.
- **L'intégrité :** Il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. L'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.
- **La disponibilité :** Il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment. La disponibilité d'un équipement se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.

- **La non-répudiation :** Une transaction ne peut être niée par aucun des correspondants. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues. Cela se fait par le biais de certificats numériques grâce à une clé privée.

- **L'authentification :** Elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

II.3.1 RISQUES ET MENACES

Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi. Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés.

L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque. On obtient ainsi la liste de ce qui doit être protégé. Il faut cependant prendre conscience que les principaux risques restent : câble arraché, coupure secteur, crash disque, mauvais profil utilisateur ...

Voici quelques éléments pouvant servir de base à une étude de risque :

- Quelle est la valeur des équipements, des logiciels et surtout des informations ;
- Quel est le coût et le délai de remplacement ;
- Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau (programmes d'analyse des paquets, logs...) ;
- Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société.

En fait, avec le développement de l'utilisation d'internet, nombre d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, elles sont plus au niveau de l'architecture trois tiers ou un-tiers. Il devient donc nécessaire de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système. En revanche, la sécurité est un compromis entre coûts, risques et contraintes. On comprendra mieux le poids d'un risque en se fiant à la formule suivante

$$\textbf{Risque} = \frac{\textbf{Menace x Vulnerabilite}}{\textbf{Contre mesure}}$$

- **Risque :** C'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit, c'est une possibilité qu'un fait dommageable se produise.
- **Vulnérabilité :** C'est une faiblesse inhérente à un système (software ou hardware). Appelée parfois faille, elle représente le niveau d'exposition face à la menace dans un contexte particulier.
- **Menace :** C'est le danger (interne ou externe) tel qu'un hacker, un virus, etc.
- **Contre-mesure :** C'est un moyen permettant de réduire le risque dans une organisation

II.4 TYPES D'ATTAQUE

Une attaque peut être classée par son comportement ou par la position de l'attaquant.

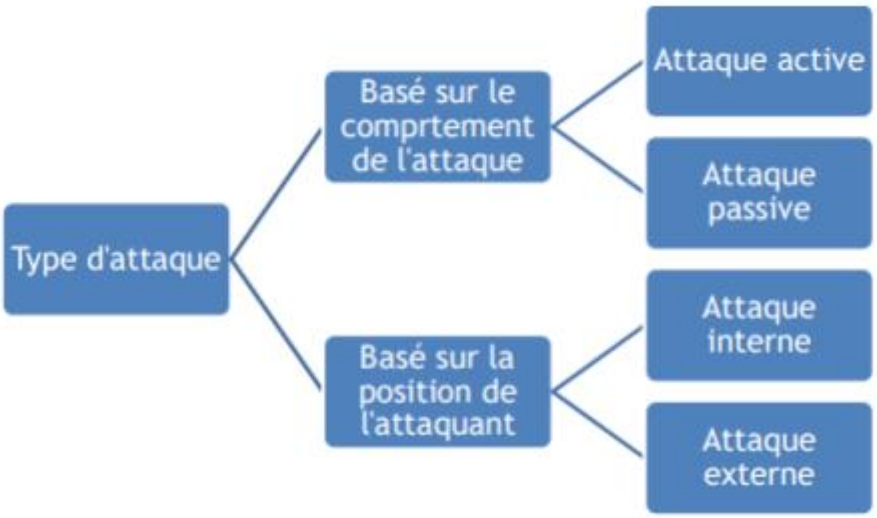


Figure 1 : Types d'attaque

II.4.1 BASE SUR LE COMPORTEMENT DE L'ATTAQUE

II.4.1.1 Attaque Active

Une attaque active est un type d'attaque informatique où l'attaquant interagit directement avec les données ou les systèmes en cours d'utilisation, souvent dans le but de modifier, d'intercepter ou de détruire des informations.

Voici quelques types d'attaque Active

- **Attaque masquée**

Lors d'une attaque par dissimulation, l'intrus se fait passer pour un utilisateur particulier d'un système afin d'y accéder ou d'obtenir des privilèges supérieurs à ceux auxquels il est autorisé.

- **Attaque de détournement de session**

Une attaque de détournement de session est également appelée attaque par relecture de session. Dans ce cas, l'attaquant exploite une vulnérabilité d'un réseau ou d'un système informatique et rejoue les informations de session d'un système ou d'un utilisateur précédemment autorisé.

- **Attaque par modification de message**

Lors d'une attaque par modification de message, un intrus modifie les adresses d'entête de paquet pour diriger un message vers une destination différente ou pour modifier les données sur une machine ciblent.

- **Attaque DoS**

Lors d'une attaque par déni de service (DoS), les attaquants submergent le système, le réseau ou le site Web de la victime avec du trafic réseau, ce qui rend difficile l'accès des utilisateurs légitimes à ces ressources.

- **Injection SQL**

L'attaquant insère des requêtes SQL malveillantes dans une application pour manipuler la base de données.

- **Attaques Man-in-the-Middle (MitM)**

L'attaquant intercepte et éventuellement modifie les communications entre deux parties, sans qu'elles ne s'en aperçoivent.

- **Spoofing**

Usurpation d'identité d'un utilisateur ou d'un système pour accéder à des ressources protégées.

- **Exploitation de vulnérabilités**

Utilisation de failles de sécurité dans des logiciels ou des systèmes pour exécuter du code malveillant ou accéder à des ressources

II.4.1.2 **Attaque Passive**

Une attaque passive est un type d'attaque informatique où l'attaquant intercepte ou surveille les communications ou les données sans interférer directement avec leur fonctionnement.

Voici quelques types d'attaque Passive

- **Sniffing**

Utilisation d'outils pour intercepter et analyser le trafic réseau. Cela peut inclure des informations non chiffrées comme des mots de passe et des messages.

- **Eavesdropping**

Écoute clandestine des communications, que ce soit par téléphone, chat ou autre moyen, pour recueillir des informations.

- **Analyse de trafic**

Surveillance du trafic réseau pour détecter des modèles et extraire des informations sensibles.

- **Replays d'attaque**

Capturer des données de transmission (comme des requêtes de connexion) et les rejouer pour accéder à des systèmes, sans modifier les données à l'origine.

- **Analyse des métadonnées**

Collecte d'informations sur la communication (comme l'heure, la durée, et les participants) sans accéder au contenu des messages eux-mêmes.

II.4.2 BASE SUR LA POSITION DE L'ATTAQUANT

II.4.2.1 Attaque Interne

Une attaque interne, également appelée menace interne, désigne une situation où un individu au sein d'une organisation (comme un employé, un contractuel ou un partenaire) exploite son accès aux systèmes ou aux données pour nuire à l'organisation. Ces attaques peuvent être motivées par divers facteurs, tels que la colère, la vengeance, l'appât du gain ou l'insatisfaction au travail.

Voici quelques types d'attaque interne

- **Vol de données**

Extraction ou copie non autorisée d'informations sensibles, comme des données clients ou des secrets commerciaux.

- **Sabotage**

Altération ou destruction délibérée de données ou de systèmes pour nuire à l'organisation.

- **Fraude**

Utilisation d'accès non autorisé pour commettre des actes frauduleux, comme des détournements de fonds.

- **Divulgation d'informations confidentielles**

Partage d'informations sensibles avec des parties externes, souvent pour des gains personnels.

- **Attaque interne malveillantes**

Une attaque interne malveillante est un événement planifié, impliquant généralement un collaborateur actuel ou ancien mécontent ou dont le compte a été compromis, et qui cible l'entreprise à des fins de gains financiers personnels ou par vengeance.

- **Attaque internes dues à la négligence**

Une attaque interne due à la négligence a pour origine une erreur humaine, une imprudence ou une manipulation. Comme ces attaques ne sont pas le fait de personnes agissant de mauvaise foi, presque tout le monde peut devenir un utilisateur interne négligent.

- **Attaque interne d'accès physique**

Il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :

- Coupure de l'électricité
- Extinction manuelle de l'ordinateur
- Vandalisme
- Ouverture du boîtier de l'ordinateur et vol de disque dur
- Ecoute du trafic sur le réseau

[3]

- **Attaque interne d'interception de communications**
  - Vol de session (session hijacking)
  - Usurpation d'identité
  - Détournement ou altération de messages
- **Attaque interne d'ingénierie sociale**

Dans la majeure partie des cas le maillon faible est l'utilisateur lui-même ! En effet c'est souvent lui qui, par méconnaissance ou par duperie, va ouvrir une brèche dans le système, en donnant des informations (mot de passe par exemple) au pirate informatique ou en exécutant une pièce jointe.

- **Attaque interne trappes**

Il s'agit d'une porte dérobée (en anglais backdoor) dissimulée dans un logiciel, permettant un accès ultérieur à son concepteur.

II.4.2.2 **Attaque Externe**

Dans le domaine de la cybersécurité, une attaque externe désigne une intrusion ou une tentative d'accès non autorisé à un système informatique depuis l'extérieur, souvent réalisée par des hackers.

- **Phishing / spear phishing**

Le phishing est un type d'attaque informatique dans laquelle l'attaquant se fait passer pour une entité de confiance et trompe ses victimes pour qu'elles cliquent sur un lien frauduleux ou révèlent des informations sensibles (mots de passe, numéros de carte de crédit).

[3] *DENI BOTA MATUBA Administration réseau L2 UWB*

- **Malware**

Logiciels malveillants, comme les virus, les ransomwares ou les chevaux de Troie, qui infectent les systèmes pour voler des données ou causer des dommages.

- **Ransomware**

Le ransomware est une attaque informatique qui prend en otage les données de sa victime. Son fonctionnement est simple mais efficace : il bloque l'accès aux données de l'utilisateur et menace de les publier ou de les supprimer à moins qu'une rançon ne soit versée.

- **les chevaux de Troie**

Les chevaux de Troie informatiques sont des programmes malveillants qui se cachent à l'intérieur de logiciels légitimes pour mieux surprendre leurs victimes

- **Attaques par Déni de Service (DoS/DDoS)**

• Description : Saturation d'un service en envoyant un volume élevé de trafic pour le rendre indisponible.

- **Exploitation de Vulnérabilités**

Utilisation de failles dans les logiciels pour obtenir un accès non autorisé ou exécuter du code malveillant.

- **Attaques Man-in-the-Middle (MitM)**

L'attaque MITM (Man-In-The-Middle), est une attaque informatique où le cybercriminel s'interpose entre deux parties qui communiquent, sans qu'elles ne se rendent compte de sa présence.

II.4.3 MECANISMES DE SECURITE EN RESEAU

Nous tenons d'abord à définir un mécanisme de sécurité, comme étant un ensemble de stratégies, conçues et mises en place pour détecter, prévenir et lutter contre une attaque.

Avec l'évolution de la technologie, il existe une panoplie de mécanismes de sécurité. Nous ne saurons, cependant, les évoquer en intégralité dans notre travail donc nous devons illustre quelques-unes :

- **Bourrage de trafic**

Données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.

- **Contrôle d'accès**

Vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité.

- **Contrôle d'accès aux communications**

Le moyen de communication n'est utilisé que par des acteurs autorisés. Par VPN ou tunnels.

- **Distribution de clefs**

Distribution sécurisée des clefs entre les entités concernées.

- **L'authentification**

Est un mécanisme de sécurité qui consiste à assurer l'identité d'un utilisateur, ou d'une machine voulant accéder au système, ainsi on vérifie que la station ou la personne, est bien celle qu'elle prétend être. En effet dans la plupart de temps, l'authentification s'agit du couple « nom d'utilisateur/mot de passe », c'est un mécanisme qui constitue une sécurité relativement fiable lorsqu'il est bien mis en œuvre. Ce mécanisme pose tout de même certains problèmes, comme par exemple, le cas où un utilisateur a besoin de se connecter sur plusieurs stations différentes, dans ce cas ce mécanisme devient relativement lourd Le mécanisme d'authentification permettant un niveau de sécurité élevé, est celui qui fait appel à un serveur d'authentification, qui centralise, géré et contrôle tous les accès aux ressources du système, c'est le mécanisme que, nous allons implémenter dans notre travail.

- **Le cryptage ou le chiffrement des données**

C'est aussi un mécanisme de sécurité, qui consiste à traduire un message clair, dit originel en un message incompréhensible, inintelligible. Le résultat du processus de cryptage est appelé « texte chiffré ou message codé », le processus de cryptage reposent à la fois sur des algorithmes puissants et sur les paramètres appelés clés, c'est ainsi que les techniques de cryptographie sont essentiellement scindées en deux.

II.5 MISE EN PLACE D'UNE POLITIQUE DE SECURITE RESEAU

II.5.1 DEFINITION

Une politique de sécurité réseau est un document générique qui définit les règles à suivre pour les accès au réseau informatique et pour les flux autorisés ou non, détermine comment les politiques sont appliquées et présente une partie de l'architecture de base de l'environnement de sécurité du réseau. La mise en place d'une politique de sécurité adéquate est essentielle à la bonne sécurisation des réseaux et systèmes d'information.

II.5.2 OBJECTIF D'UNE POLITIQUE DE SECURITE

La définition d'une politique de sécurité n'est pas un exercice de style, mais une démarche de toute l'entreprise visant à protéger son personnel et ses biens d'éventuels incidents de sécurité dommageables pour son activité. La définition d'une politique de sécurité réseau fait intégralement partie de la démarche sécuritaire de l'entreprise. Elle s'étend à de nombreux domaines, dont les suivants :

- Audit des éléments physiques, techniques et logiques constituant le système d'information de l'entreprise.

- Sensibilisation des responsables de l'entreprise et du personnel aux incidents de sécurité et aux risques associés.
- Formation du personnel utilisant les moyens informatiques du système d'information.
- Structuration et protection des locaux abritant les systèmes informatiques et les équipements de télécommunication, incluant le réseau et les matériels.
- Ingénierie et maîtrise d'œuvre des projets incluant les contraintes de sécurité dès la phase de conception.
- Gestion du système d'information de l'entreprise lui permettant de suivre et d'appliquer les recommandations des procédures opérationnelles en matière de sécurité.
- Définition du cadre juridique et réglementaire de l'entreprise face à la politique de sécurité et aux actes de malveillance, 80% des actes malveillants provenant de l'intérieur de l'entreprise.
- Classification des informations de l'entreprise selon différents niveaux de confidentialité et de criticité.

II.5.3 **LES DIFFERENTS TYPES DE POLITIQUE DE SECURITE**

Une politique de sécurité réseau couvre les éléments suivants :

- **Sécurité de l'infrastructure**

La sécurité de l'infrastructure couvre la sécurité logique et physique des équipements et des connexions réseaux, aussi bien internes que celles fournies par des fournisseurs d'accès internet (FAI).

- **Sécurité des accès**

La sécurité d'accès couvre la sécurité logique des accès locaux et distants aux ressources de l'entreprise, ainsi que la gestion des utilisateurs et de leurs droits d'accès au système d'informations de l'entreprise.

- **Sécurité du réseau intranet face à Internet ou aux autres** parties

La sécurité du réseau intranet face à Internet ou aux autres parties couvre la sécurité logique des accès aux ressources de l'entreprise (Intranet) et l'accès aux ressources extérieures (Extranet).

N.B : la définition d'une politique de sécurité réseau vise à la fois à définir les besoins de sécurité de l'entreprise, à élaborer des stratégies de sécurité afin de protéger les biens les plus critiques et à définir le référentiel des contrôles de sécurité.

II.6 **LES STRATEGIES DE LA SECURITE**

Après avoir défini les objectifs et les différents types de politiques de sécurité réseau, nous détaillons à présent les stratégies de sécurité à adopter pour mettre en œuvre une telle politique. La conception de stratégies de sécurité exige de prendre en compte l'historique de l'entreprise, l'étendue de son réseau, le nombre d'employés, la sous-traitance avec des tierces parties, le nombre de serveurs, l'organisation du réseau, etc. D'une manière générale, une bonne stratégie de sécurité vise à définir et à mettre en œuvre des mécanismes de sécurité,

des procédures de surveillance des équipements de sécurité, des procédures de réponse aux incidents de sécurité et des contrôles et audits de sécurité. Elle veille en outre à ce que les dirigeants de l'entreprise approuvent la politique de sécurité de l'entreprise.

II.6.1 METHODOLOGIE POUR ELABORER UNE POLITIQUE DE SECURITE RESEAU

Diverses méthodes permettent d'élaborer des stratégies de sécurité. Nous décrivons ici la méthodologie générique à savoir :

- **Prédiction des attaques potentielles et analyse de risque**

La première étape consiste à déterminer les menaces qui pèsent sur les biens de l'entreprise, ainsi que les impacts de ces menaces sur l'activité de l'entreprise si elles devaient se concrétiser. Le rapprochement entre les ressources critiques de l'entreprise et les risques de sécurité associés, déterminés par le triptyque menace/vulnérabilité/conséquence, permet de définir la stratégie sécurité de l'entreprise. Afin de protéger ses biens critiques des menaces identifiées, l'entreprise doit aussi analyser les techniques d'attaque utilisées pour enfreindre les contrôles de sécurité ou tirer parti des vulnérabilités.

- **Analyse des résultats et amélioration des stratégies de sécurité**

Les différentes simulations sont l'occasion d'améliorer les contre-mesures de sécurité, voire de les remettre en question. Par exemple, si l'on constate que certains types d'attaques ne sont pas détectés par un pare-feu, les règles de filtrage définies ou le pare-feu lui-même doivent être remis en cause. Il faut aussi valider l'efficacité des stratégies de sécurité mises en place face aux simulations exécutées. Enfin, dans la mesure où la stratégie existante n'a pas apporté de résolution satisfaisante, il est nécessaire de la modifier ou d'en créer une nouvelle.

- **Règles élémentaires d'une stratégie de sécurité réseau**

Lors de la conception d'une stratégie de sécurité, il faut toujours garder à l'esprit quelques règles ou principes élémentaires afin de se prémunir des erreurs possibles dans le choix de contre-mesures. Voici quelques-uns :

  - **Simplicité** : Plus une stratégie n'est complexe, plus il est difficile de l'appliquer, de la maintenir dans le temps ou de la faire évoluer. La simplicité et le pragmatisme sont des critères de réussite d'une stratégie de sécurité.
  - **Le maillon le plus faible :** Un réseau est composé d'un ensemble d'équipements, ayant ou non une fonction de sécurité implémentée. Pour qu'une stratégie de sécurité recouvre le périmètre de l'entreprise, il faut s'assurer que toutes les méthodes d'accès fournissent un même niveau de sécurité, faute de quoi le maillon le plus faible sera privilégié pour attaquer le réseau d'entreprise.
  - **Variété des protections** : La variété des solutions mises en place pour assurer la sécurité ne doit pas se fonder sur un seul type de logiciel de pare-feu ou de détection d'intrusion ;
  - **L'implémentation en profondeur des mécanismes de sécurité :** La sécurité ne doit jamais reposer sur un seul mécanisme de sécurité. Une

imbrication de mécanismes offre une garantie de sécurité bien supérieure, pour peu que le premier élément de sécurité vienne à faillir. L'implémentation de mécanismes de sécurité en profondeur doit être comprise et perçue comme une assurance de sécurité à plusieurs niveaux. Plus le système à protéger est critique, plus le nombre de mécanismes de sécurité ne doit être important.

II.6.2 METHODOLOGIE POUR ELABORER UNE POLITIQUE DE SECURITE INFORMATIQUE

Élaborer une politique de sécurité informatique est essentiel pour protéger les actifs informationnels d'une organisation. Voici une méthodologie en plusieurs étapes pour vous guider dans ce processus :

- **Analyse du contexte**

  - **Évaluer les besoins** : Comprendre pourquoi une politique de sécurité est nécessaire.
  - **Identifier les parties prenantes** : Impliquer la direction, le personnel IT, et d'autres utilisateurs clés.

- **Évaluation des risques**

  - **Identifier les actifs** : Cataloguer les informations et les systèmes critiques.
  - **Analyser les menaces** : Identifier les menaces potentielles (piratage, malware, erreurs humaines, etc.).
  - **Évaluer les vulnérabilités** : Analyser les faiblesses des systèmes et des processus.
  - **Estimer les impacts** : Évaluer les conséquences potentielles d'une violation de la sécurité.

- **Définition des objectifs de sécurité**

  - **Confidentialité** : Protéger les informations sensibles.
  - **Intégrité** : Assurer que les informations ne sont ni altérées ni détruites de manière non autorisée.
  - **Disponibilité** : Garantir l'accès aux informations et systèmes lorsque nécessaire.

- **Rédaction de la politique**

  - **Établir des directives claires** : Définir les comportements attendus des utilisateurs et les mesures de sécurité à mettre en place.
  - **Inclure des procédures** : Détailler les procédures pour la gestion des incidents, la gestion des accès, et la sauvegarde des données.
  - **Préciser les rôles et responsabilités** : Définir qui est responsable de la mise en œuvre et du respect de la politique.

- **Sensibilisation et formation**

  - **Former le personnel** : Organiser des sessions de sensibilisation pour informer les employés sur la politique et les bonnes pratiques en matière de sécurité.

- **Promouvoir une culture de sécurité** : Encourager un comportement proactif en matière de sécurité au sein de l'organisation.

- **Mise en œuvre**

  - **Déployer des contrôles techniques** : Installer des outils de sécurité (pare-feu, antivirus, cryptage, etc.).
  - **Établir des mécanismes de surveillance** : Mettre en place des systèmes pour détecter et répondre aux incidents de sécurité.

- **Révision et mise à jour**

  1. **Évaluer régulièrement la politique** : Effectuer des audits pour s'assurer que la politique est toujours pertinente et efficace.
  2. **Mettre à jour la politique** : Adapter la politique en fonction des évolutions technologiques, des nouvelles menaces et des retours d'expérience.

- **Documentation et communication**

  - **Documenter la politique** : Rédiger un document formel qui décrit la politique de sécurité.
  - **Communiquer efficacement** : S'assurer que la politique est facilement accessible à tous les employés et qu'ils en comprennent les implications.

II.7 **PROPOSITION DE STRATEGIES DE SECURITE RESEAU**

Pour proposer une bonne stratégie de sécurité, il faut procéder étape par étape en prenant en compte les éléments suivants :

II.7.1 **STRATEGIE DES PERIMETRES DE SECURITE**

Le réseau d'entreprise est découpé en périmètres de sécurité logiques regroupant des entités ou fonctions afin de mettre en place des niveaux de sécurité à la fois imbriqués et séparés. On définit un périmètre autour du réseau d'entreprise (intranet) face au réseau Internet. Nous définissons également des périmètres de sécurité pour chacun des sous-réseaux inclus dans le réseau intranet. L'objectif est de compartimenter le réseau et de créer une imbrication des périmètres de sécurité afin de rendre plus difficile une pénétration éventuelle.

II.7.1.1 **Stratégie des goulets d'étranglement**

Des contrôles d'accès différenciés et en nombre limité sont implémentés pour permettre l'accès à chaque périmètre de sécurité du réseau de l'entreprise. Les contrôles d'accès définissent ce qui est autorisé à rentrer ou à sortir d'un périmètre de sécurité. Nous partons du postulat que « tout ce qui n'est pas autorisé est interdit ». Les contrôles d'accès définissent par ailleurs les conditions à respecter pour avoir le droit d'entrer dans le périmètre de sécurité.

II.7.1.2 **Stratégie d'authentification en profondeur**

Des contrôles d'authentification sont mis en place afin d'authentifier les accès aux périmètres de sécurité. Dans cette stratégie, des systèmes de contrôle d'authentification sont insérés au sein d'un périmètre de sécurité. Les contrôles d'authentification des utilisateurs s'effectuent à plusieurs passages, au niveau de la sortie Internet, où chaque utilisateur doit s'authentifier pour avoir accès à Internet, mais aussi au niveau de chaque serveur pour accéder au réseau interne (serveurs de fichiers, serveurs d'impression, etc.). Chaque fois qu'un utilisateur s'authentifie, un ticket est créé sur un système chargé de stocker les traces (logs) afin que le parcours de l'utilisateur soit connu à tout moment de manière précise. Cette logique peut être généralisée et entraîner la création d'une trace pour chaque action de l'utilisateur sur chaque serveur (création, consultation, modification, destruction de fichier, impression de document, URL visitée par l'utilisateur, etc.). On parle dans ce cas de modèle AAA (Authentication, Authorization, Accounting), autrement dit authentification, autorisation et comptabilité des événements.

La mise en place d'une telle infrastructure est toutefois lourde et coûteuse.

II.7.1.3 **Stratégie du moindre privilège**

La stratégie du moindre privilège consiste à s'assurer que chacun dispose de tous les privilèges et seulement des privilèges dont il a besoin. Par la stratégie du moindre privilège, la portée de tout acte de malveillance se trouve réduite par défaut aux privilèges dont dispose la personne qui le commet. Un moyen de renforcer à l'infini cette technique consiste à augmenter le nombre d'autorisations nécessaires afin qu'une opération soit possible. Le principe est que « Un utilisateur ne dispose que des privilèges dont il a besoin ». La mise en œuvre de ce principe simple à énoncer est assez lourde pour l'entreprise en termes de ressources et de coûts.

II.7.1.4 **Stratégie de confidentialité des flux réseau**

Tout message qui doit être émis à l'extérieur ou vers d'autres réseaux doit être protégé. Pour y parvenir, le message doit être chiffré. « Toute communication intersites transitant sur des réseaux publics est chiffrée si elle contient des données confidentielles » [8]. Cette stratégie est généralement appliquée aux réseaux d'entreprise répartis sur plusieurs sites distants communiquant entre eux par l'intermédiaire de réseaux publics tels qu'Internet, liaisons spécialisées, etc.

II.7.1.5 **Stratégie de contrôle régulier**

La stratégie de contrôle régulier consiste à simuler des tentatives de pénétration surprises afin de vérifier le bon fonctionnement des mécanismes de sécurité. « L'application de la politique de sécurité est validée par un contrôle de sécurité régulier. » Lorsque l'entreprise s'interconnecte à Internet, elle fait souvent appel à une tierce partie consultante, censée maîtriser la mise en place de ce service. Comme l'entreprise ne peut juger de la pertinence de la sécurité implémentée, elle doit faire contrôler régulièrement la sécurité par une tierce partie afin de détecter et de corriger les faiblesses de sécurité éventuelles.

Après avoir défini les politiques et stratégies de sécurité réseau, il est important de sensibiliser les utilisateurs sur l'importance du respect de la politique et stratégies de sécurité afin qu'ils soient conscients de leurs responsabilités.

II.8 **TECHNIQUE AUX PARADES DES ATTAQUES**

II.8.1 **La cryptographie**

La cryptographie permet l'échange sûr des renseignements privés et confidentiel. Un texte compréhensible est converti en texte inintelligible (chiffrement), en vue de sa transmission d'un poste de travail à un autre. Sur le poste récepteur, le texte chiffré est reconverti en format intelligible (déchiffrement). On peut également utiliser la cryptographie pour assurer l'authentification, la non-répudiation et l'intégrité de l'information, grâce à un processus cryptographique spécial appelé signature numérique. Celle-ci permet de garantir l'origine et l'intégrité de l'information échangée, et aussi de confirmer l'authenticité d'un document.

II.8.1.1 **Cryptographie symétrique**

La cryptographie à clé symétrique a très longtemps été utilisée pour le chiffrement de messages confidentiels. Son usage a été progressivement réduit depuis l'apparition de la cryptographie à clé publique (cryptographie asymétrique) même si les deux techniques sont encore parfois utilisées conjointement. Dans le chiffrement à clé symétrique ou clé secrète, c'est la même clé qui sert à la fois à chiffrer et à déchiffrer un message. C'est exactement le même principe qu'une clé de porte : c'est la même qui sert à ouvrir et à fermer une serrure.

II.8.1.2 **Cryptographie asymétrique**

La cryptographie asymétrique appelée également cryptographie à clé publique est une méthode utilisée pour transmettre et échanger des messages de façon sécurisée en s'assurant de respecter les principes suivants :

- Authentification de l'émetteur ;
- Garantie d'intégrité ;
- Garantie de confidentialité.

Cette technique repose sur le principe de « paire de clés » (ou bi-clés) composée d'une clé dite « privée » conservée totalement secrète et ne doit être communiquée à personne et d'une clé dite « publique » qui, comme son nom l'indique peut être transmise à tous sans aucune restriction. Ces deux clés sont mathématiquement liées. Dans la pratique, la clé publique sert à crypter les messages, et la clé privée sert à les décrypter. Une fois le message crypté, seul le destinataire est en mesure de le décrypter.

II.9 **SERVEUR PROXY**

II.9.1. **PRESENTATION**

Un serveur Proxy, aussi appelé serveur mandataire est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local, utilisant parfois des protocoles autre que le protocole TCP/IP et Internet. Un proxy est donc un ensemble de

processus permettant d'éliminer la connexion directe entre les applications des clients et les serveurs. La plupart du temps le serveur Proxy est utilisé pour le web, il s'agit alors d'un Proxy HTTP. Toutefois il peut exister des serveurs Proxy pour chaque protocole applicatif (FTP, etc.).

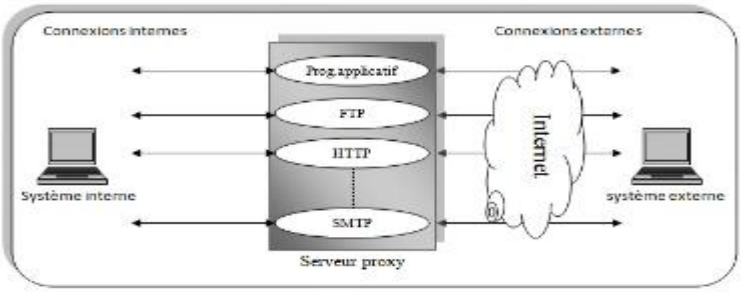


Figure 2 : Architecture d'un Proxy"

II.9.2. **PRINCIPE DE FONCTIONNEMENT**

Le principe de fonctionnement d'un serveur Proxy est assez simple : il établit en lieu et place de l'utilisateur le service invoqué par celui-ci (FTP, etc.). Ainsi lorsqu'un utilisateur se connecte à l'aide d'une application cliente configurée pour utiliser un serveur Proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur Proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête (le serveur Proxy contacte le serveur externe sollicité sur internet avec sa propre adresse ou une adresse issue d'un pool d'adresses IP libres). Le serveur va ensuite donner sa réponse au Proxy, qui va à son tour la transmettre à l'application cliente. Le Proxy cache de la sorte toute l'infrastructure du réseau local et ne dévoile en aucun cas les adresses des machines internes (masquage d'adresse).

II.9.2.1 **Fonctionnement d'un serveur Proxy**

Avec l'utilisation de TCP/IP au sein des réseaux locaux, le rôle de relais du serveur proxy est directement assuré par les passerelles et les routeurs. Les serveurs Proxys sont toujours d'actualité grâce à un certain nombre d'autres fonctionnalités.

II.9.2.2 **Cache**

La plupart des Proxys assurent ainsi une fonction de cache (caching), c'est-à-dire la capacité à garder en mémoire (en « cache ») les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les leur fournir le plus rapidement possible. En effet, en informatique, le terme de « cache » désigne un espace de stockage temporaire de données (le terme de « tampon » est également parfois utilisé). Un serveur Proxy ayant la possibilité de cacher (néologisme signifiant « mettre en mémoire cache ») les informations sont généralement appelé serveur Proxy-cache. Cette fonctionnalité implémentée dans certains serveurs Proxys permet d'une part de réduire l'utilisation de la bande passante vers Internet ainsi que de réduire le temps d'accès aux documents pour les utilisateurs. Toutefois, pour mener à bien cette mission, il est nécessaire que le Proxy compare régulièrement les données qu'il stocke en mémoire cache avec les données distantes afin de s'assurer que les données en cache sont toujours valides.

II.9.2.3 **Filtrage**

D'autre part, grâce à l'utilisation d'un Proxy, il est possible d'assurer un suivi des connections via la constitution des journaux d'activités (logs) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet. Il est ainsi possible de filtrer les connexions à internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs. Le filtrage basé sur l'adresse des ressources consultées est appelé filtrage d'URL. Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de liste blanche, lorsqu'il s'agit d'une liste de sites interdits on parle de liste noire. En fin l'analyse des réponses des serveurs conformément à une liste de critères (mots-clés…) est appelée filtrage de contenu.

II.9.2.4 **Authentification**

Dans la mesure où le Proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour authentifier les utilisateurs, c'est-à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple.

Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistrer dans les fichiers journaux des accès identifiés. Ce type de mécanisme lorsqu'il est mise en œuvre pose bien évidement de nombreux problèmes relatifs aux libertés individuelles et aux droits des personnes.

II.9.3. **REVERSE PROXY**

On appelle Reverse-Proxy (en français le terme de relais inverse est parfois employé) un serveur Proxy-cache « monté à l'inverse », c'est-à-dire un serveur Proxy permettant non pas aux utilisateurs d'accéder au réseau Internet, mais aux utilisateurs d'internet d'accéder indirectement à certains serveurs internes.

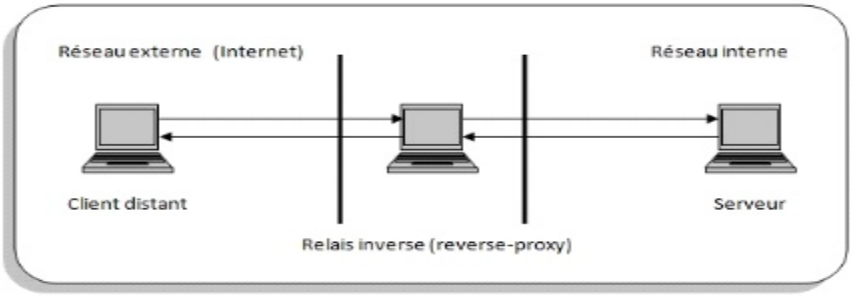


Figure 3 Reverse Proxy

Le Reverse-Proxy sert ainsi de relais pour les utilisateurs d'Internet souhaitant accéder à un site web interne en lui transmettant indirectement les requêtes. Grâce au Reverse-Proxy, le serveur web est protégé des attaques directes de l'extérieur, ce qui renforce la sécurité du réseau interne. D'autre part, la fonction du cache du reverse-Proxy peut permettre de soulager la charge du serveur pour lequel il est prévu, c'est la raison pour laquelle un tel serveur est parfois appelé « accélérateur », (server accelerator). Enfin, grâce à des algorithmes perfectionnés, le Reverse-Proxy peut servir à répartir la charge en redirigeant les requêtes vers différents serveurs équivalents ; on parle alors de répartition de charge, (load balancing).

II.10 **PARE-FEU**

Un pare-feu, (appelé aussi Coupe-feu, Garde-barrière) l'anglais « firewall », est un logiciel et/ou un matériel qui inspecte les paquets entrants et sortants du réseau afin d'autoriser ou d'interdire leur passage en se basant sur un ensemble de règles appelées ACL (« Access Control List »). Il enregistre également les tentatives d'intrusions dans un journal transmis aux administrateurs du réseau et permet de contrôler l'accès aux applications et d'empêcher le détournement d'usage. Un pare-feu dans un réseau a pour but de déterminer le type de trafic qui sera acheminé ou bloqué, de limiter le trafic réseau et accroître les performances, contrôler le flux de trafic, fournir un niveau de sécurité d'accès réseau de base, autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau, filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau. Il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau (cartes réseau) suivantes :

- Une interface pour le réseau à protéger (réseau interne) ;
- Une interface pour le réseau externe.

II.11 **CONCLUSION**

En conclusion, face à la complexité croissante des menaces et à la sophistication des techniques d'attaque, il est impératif de mettre en place une approche de sécurité holistique et proactive qui couvre tous les aspects de l'infrastructure réseau. Cela implique non seulement l'utilisation de technologies de sécurité avancées, mais aussi une gestion des risques, une planification de la continuité des activités, et une culture de sécurité bien ancrée au sein de l'organisation. La résilience face aux attaques réseau repose sur une préparation rigoureuse et une capacité de réponse rapide aux incidents.

Chap III **CADRAGE DU PROJET**

III.1 **INTRODUCTION**

Il est difficile de parler d'un projet avant d'avoir fait une analyse détaillée du travail à faire. Il est cependant nécessaire d'effectuer une première estimation générale pour pouvoir délimiter ce projet.

Dans ce chapitre nous allons mettre l'accent sur l'aspect du cadrage du projet et faire une étude détaillée du projet.

III.2 **LA DEFINITION DU PROJET**

Un projet est un processus unique, qui consiste en un ensemble d'activités coordonnées et maitrisées comportant des dates de début et de fin, l'entreprise dans le but d'attendre un objectif conforme à des exigences spécifiques telles que des contraintes des délais, de couts et de ressources.

III.3 **PRESENTATION**

Le présent projet c'est la mise en place d'un réseau informatique dans une entreprise multi site qui fera à ce que ses différents sites soient reliés grâce au réseau informatique que nous allons mettre en place malgré leurs distances.

III.4 **IMPORTANCE DU PROJET**

Ce projet a comme importance :

- Il permet de ne pas interrompre la chaîne numérique,
- D'automatiser,
- De standardiser,
- Et de centraliser certaines tâches.

III.5 **CAHIER DE CHARGE**

Le cahier des charges est un document contractuel qui permet au maitre d'ouvrage de faire savoir au maitre d'œuvre ce qu'il attend de lui lors de la réalisation d'un projet, entrainant des pénalités en cas de non-respect. Il décrit précisément les besoins auxquels le prestataire ou le soumissionnaire doit répondre, et organise la relation entre les différents acteurs tout au long du projet.

En tant que pièce de référence du contrat, le cahier des charges protège les deux parties de toute ambiguïté : le maitre d'ouvrage est assuré que la livraison sera conforme à ses attentes, tandis que le maitre d'œuvre peut mener à bien le projet sans subir de jugements intempestifs au fur et à mesure. Toutefois, le maitre d'ouvrage a la possibilité de modifier le cahier des charges en cours de route au travers d'un avenant accepté par le maitre d'œuvre.

III.5.1 **CONTACT**

Pour la réalisation de notre projet nous avons eu à contacter les dirigeants de l'entreprise (MENZIES) pour leurs montrent la valeur de notre projet au sein de leur entreprise.

III.5.2 **OBJECTIF A REALISER**

Notre projet repose sur trois objectifs principaux, à savoir :

- Objectifs techniques : les résultats attendus et du projet
- Objectif de délai : un chronogramme fixant la date et la fin du projet ainsi que celle des différents étapes sa mise en œuvre
- Objectifs du cout : le cout raisonnable pour réaliser ce projet.

III.5.3 **CONTRAINTES**

Il y a trois contraintes qui sont liée au projet à savoir :

- **Contrainte du cout (budget**) : tout le monde doit être satisfait, si un geste commercial est envisagé, il ne doit surtout pas impacter le nombre de jours estimé et donc le planning. Outre le geste commercial, la simplification du cahier des charges (souvent très vaste) peut être envisagée : moins de développement, moins de test, moins de suivi donc forcément un coût moins élevé.
- **Contrainte des temps (début et fin)** : dans le cadre de ce projet nous nous proposons, le découpage en lots ainsi que les méthodologies agiles peuvent permettre de respecter les délais. De plus, il ne faut pas se tirer une balle dans le pied en avant-vente, les clients sont comme les enfants, ils sont impatients de voir leur nouveau joujou au plus vite, mais rien n'empêche d'entamer une discussion et de gagner quelques semaines quitte à livrer une première version simplifiée.
- **Contrainte techniques (qualité du résultat)** : la transparence avec MENZIES est de mise pour, optimiser les processus de production et mettre en place une réelle phase de recette en prévoyant également une période de garantie et de TMA (Tierce Maintenance Applicative).

III.5.4. **STRUCTURE GENERALE A REALISER**

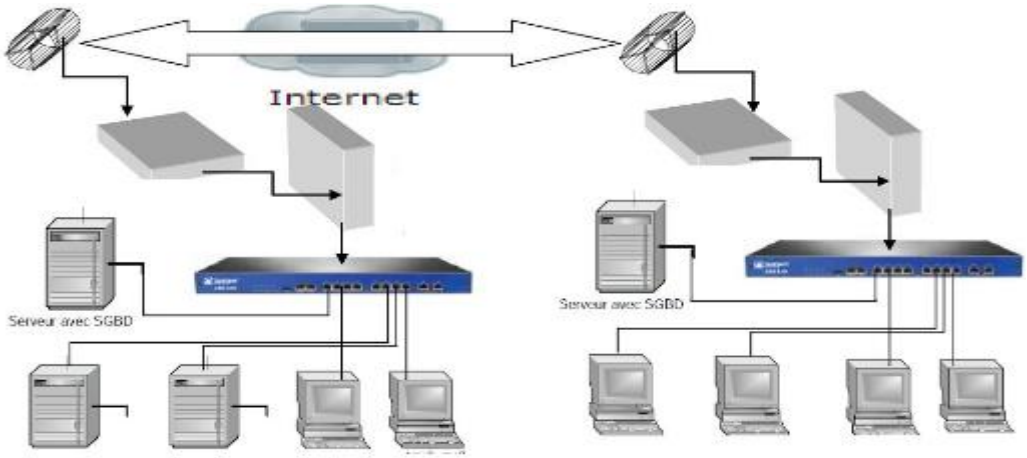


Figure 4 structure générale a réaliser

III.6 **PLANIFICATION D'ORDONNANCEMENTS**

III.6.1. **INTRODUCTION**

La construction du planning d'un projet passe par la modélisation d'un réseau de dépendance entre tâches sous forme graphique. Il s'agit d'une décomposition structurée du travail. Il faut décomposer le projet en sous-ensembles plus simples

Les méthodes d'ordonnancement des tâches permettent d'avoir une représentation graphique (immuable ou non) d'une réalisation en représentant chaque opération (ou tâche) par un arc, une liaison, ou un rectangle qui peut être proportionnel ou non à la durée. Ce graphique dans tous les cas, permet le positionnement relatif des opérations dans le temps.

III.6.2 **METHODES D'ORDONNANCEMENTS**

La réalisation d'un projet nécessite souvent une succession de taches auxquelles s'attachent certaines contraintes : de temps, d'antériorité et de production.

Les méthodes d'ordonnancements (tec-hniques) dans le cadre de la gestion d'un projet ont pour objectif de répondre au mieux aux besoins exprimés par un client, au meilleur cout et dans les meilleurs délais, en tenant compte des différentes contraintes. Il existe trois méthodes d'ordonnancement, à la base de toute construction d'un projet :

- Le diagramme de GANTT
- La méthode MPM (méthode des potentiels Métra)
- La méthode PERT (program Evaluation Reviewtechnic)

- **Diagramme de GANTT**

Le diagramme de Gantt est la technique de représentation graphique permettant de renseigne et situer dans le temps les phases, activités, tâches et ressources du projet.

En ligne, on liste les tâches et en colonne les jours, semaine ou mois. Les tâches sont représentées par des barres dont la longueur est proportionnelle à la durée estimée. Les tâches peuvent se succéder ou se réaliser en parallèle entièrement ou particulièrement, ce diagramme a été conçu par un certain Henry L. GANTT (en 1917) et est encore aujourd'hui la représentation la plus utilisée.

- **Méthode PERT (programme évaluation review technique)**

La méthode PERT est une technique américaine de modélisation de projet. Elle consiste à mettre en ordre sous forme de réseau plusieurs taches qui grâce à leurs dépendances et à leur chronologie permettent d'avoir un produit fini.

- Les caractéristiques de PERT sont les suivantes :
- Les taches sont représentées par des flèches ;
- Le réseau visualise de dépendances entre tache ;
- Limite de la technique PERT : pas de représentation de notion de durée et de date
- Chaque tâche est représentée par un arc, auquel on associe un chiffre entre parenthèses ;

Entre les arcs figurent des cercles appelés « sommets » ou « évènements » qui marquent l'aboutissement d'une ou plusieurs taches. Ces cercles sont numérotés afin de suivre l'ordre de succession des divers évènements.

- **Méthode MPM**

Cette méthode a été développée par une équipe de chercheur français.

Les caractéristiques du MPM sont les suivantes :

- Les tâches sont représentées par des sommets et contrainte de succession par des sommets.
- Chaque tâche est renseignée par date- à laquelle elle peut commencer (date au plutôt) et celle à laquelle, elle doit se terminer (date au plus tard).
- A chaque arc est associée une valeur numérique, qui représente soit une durée d'opération (activité) soit un délai.

III.6.3 CHOIX DE LA METHODE

Dans le cadre de notre travail, nous choisissons la méthode PERT (Program Evaluation and ResearchTask ou Program Evaluation and ReviewTechnic). Il permet de mettre en ordre sous la forme d'un graphe, plusieurs tâches qui grâce à leur dépendance et à leur chronologie concoure nt tous à la réalisation de notre projet.

III.6.4 INVENTAIRE DES TACHES

Dans notre travail, nous avons recensé quelques tâches qui feront l'objet de notre évaluation, à savoir :

- Cadrage du projet ;
- Etude préalable ;
- Analyse détaillée ;
- Analyse technique ;
- conditionnement des équipements ;
- Acquisition du pare feu ;
- Formation des utilisateurs ;
- installation du pare feu,
- Configuration du pare feu,
- Test et correction des erreurs,
- mise en œuvre.

III.7 TABLEAU D'ANTERIORITE

Le recours à la Méthode des Potentiels Métra suppose qu'aient été identifiées préalablement les différentes tâches nécessaires à la réalisation du projet, leur durée et leurs relations d'antériorité.

Ces indications sont synthétisées dans ce tableau

Taches	Activités	Durée	Antériorités
A	Cadrage du projet	10 jours	-
B	Etude préalable	15 jours	A
C	Analyse détaillée	25 jours	B
D	Analyse technique	20 jours	C
E	Conditionnement des locaux	6 jours	D
F	Acquisition des matériels	20 jours	D
G	Formation des utilisateurs	8 jours	E, F
H	Installation du pare feu	6 jours	G
I	Configuration du pare feu	15 jours	G
J	Test et correction des erreurs	10 jours	H, I
K	Mise en œuvre	5 jours	J

Tableau : TABLEAU D'ANTERIORITE

Construction de graphe MPM

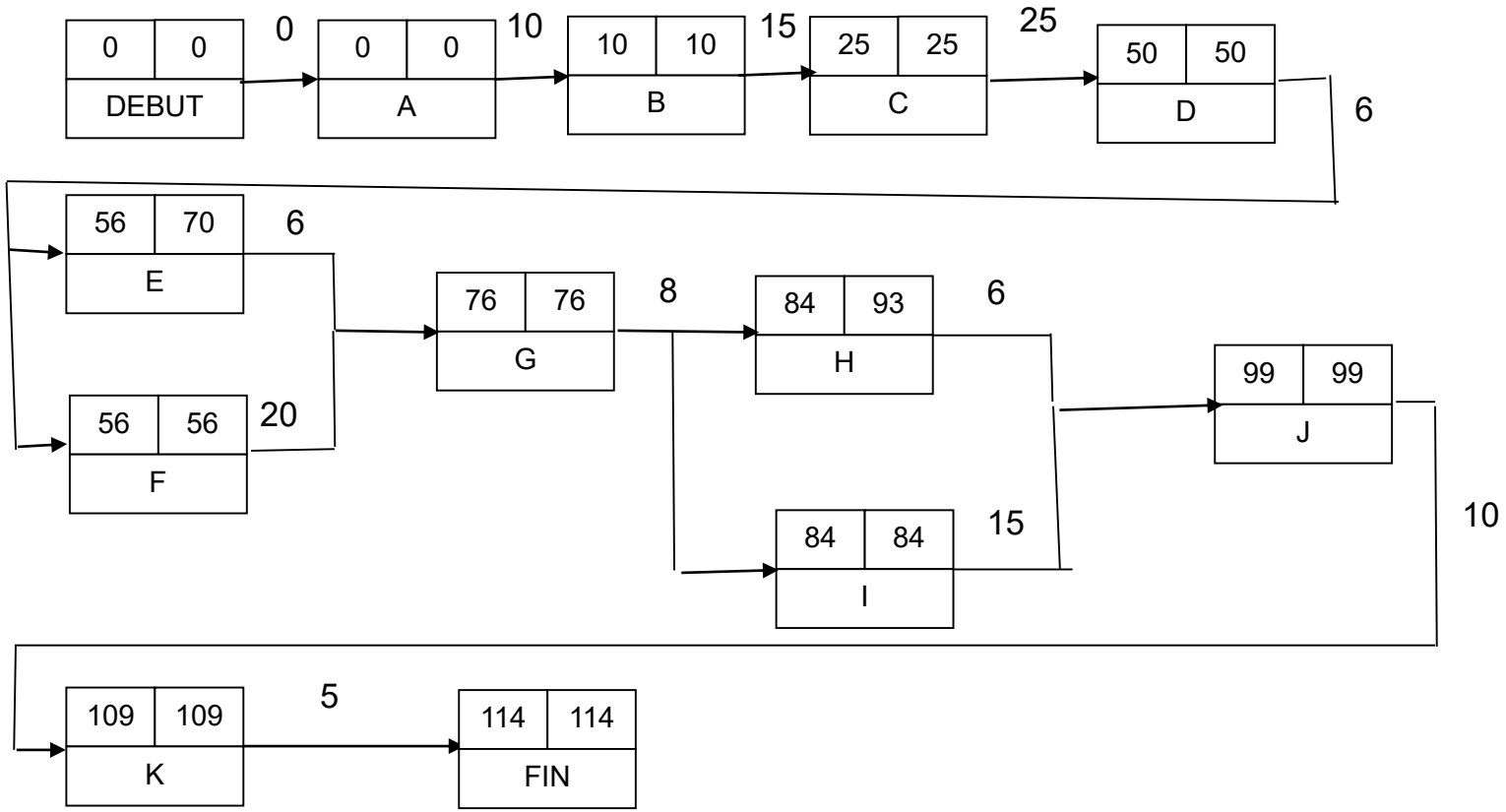


Tableau Construction de graphe MPM

Détermination du chemin critique

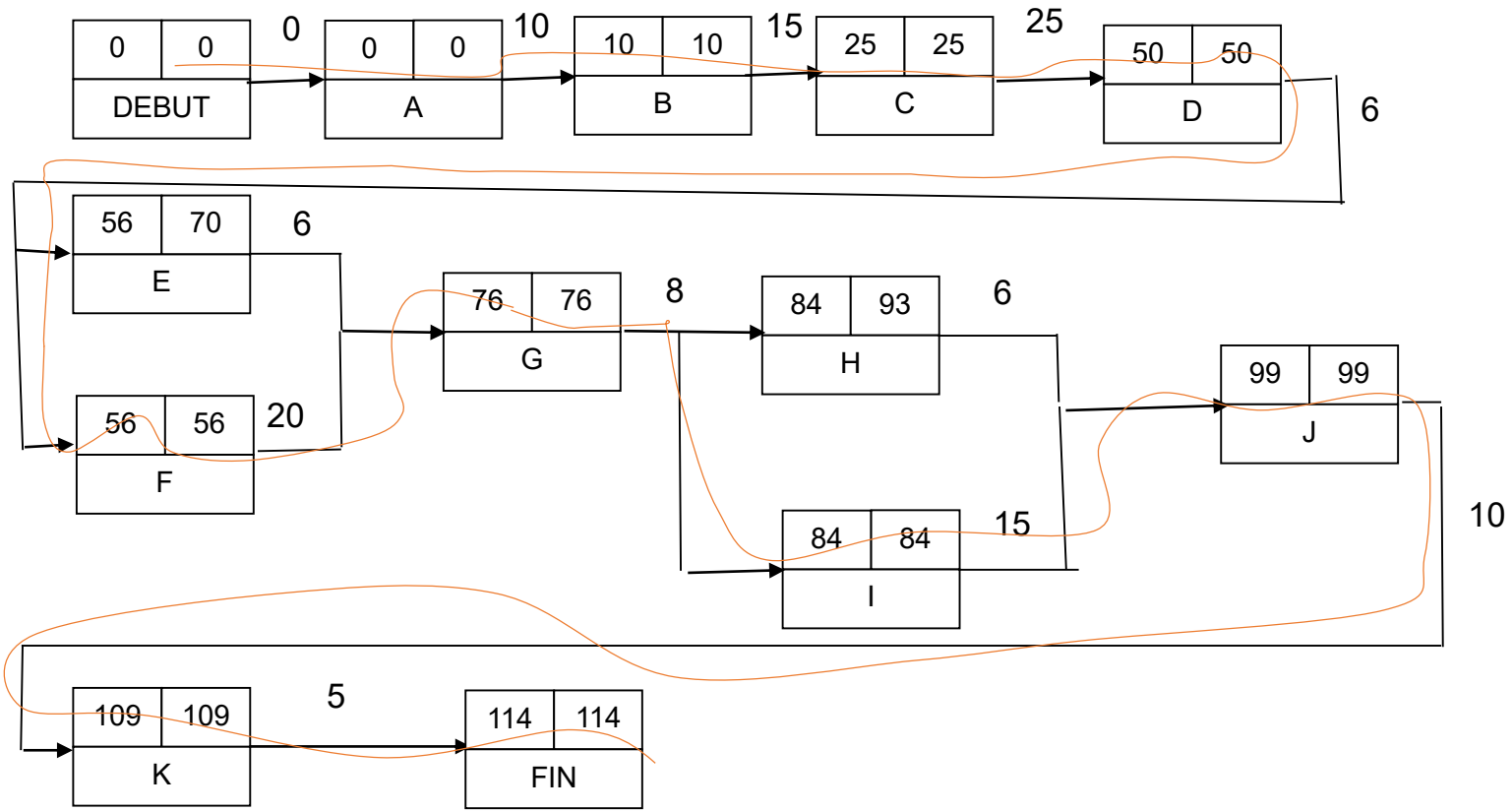


Tableau : Détermination du chemin critique

Donc notre chemin critique (C.C) : C.C = A, B, C, D, F, G, I, J, K

DUREE TOTAL

=d(A) + d(B) + d(C) + d(D) + d(E) + d(G) + d(H) + d(J) + d(K) + d(L)

= 10+15+25+20+6+8+6+10+5

=105

III.8 **COUT**

Le tableau ci-dessous nous donne le coût des activités selon leurs contraintes.

Taches	**Activités**	**Durée**	**Couts**
A	Collecte des données	10	250$
B	Analyse du système	15	300$
C	Conception du nouveau système	25	500$
D	Implémentation du pare feu	20	600$
E	Aménagement de locaux	6	700$
F	Acquisition des matériels et mise en place	20	360$
G	Installation du pare feu	8	1000$
H	Configuration du feu	6	1000$
I	Correction des erreurs	15	150$
J	Formation des utilisateurs	10	800$
K	Lancement du système	5	800$

Tableau. II.2. Coût projet

Le Coût Total de l'évaluation du projet est la sommation des coûts des toutes s tâches ou activités critiques ou non critiques, soit :

CTE =250+300+500+600+700+360+1000+1000+150+800+800

=6 460 $

III.9 **CONCLUSION**

Nous voici à la fin de notre troisième chapitre, qui nous a permis de faire une évaluation de notre projet. Et ce chapitre nous a permis de faire la présentation du projet, de montrer l'importance du projet, d'établir le cahier de charge, de montrer les objectifs à réaliser, de nous montrer encore le types de méthode d'ordonnancement ainsi que les le contraintes qui sont liée pour au projet.

CHAP IV **ETUDE DU SITE MENZIES**

IV.1 **INTRODUCTION**

Ce chapitre va nous parlent de la présentation de l'entreprise, Mission et objectif, Emplacement géographique, L'organigramme, fonctionnement et poste, Architecture de L'existant

IV.2 **PRESENTATION DE L'ENTREPRISE**

MENZIES est une compagnie d'assistance fournisseur de services aériens qui connaît la plus forte croissance sur les marchés émergents. Depuis le début de ses opérations au Édimbourg en 1833, MENZIES s'est rapidement transformé en leader de la prestation de services aériens grâce à sa présence dans +65 pays au monde et dans +250 sites. Les 8 000 employés compétents et agréables formant le cœur de son réseau mondial se sont engagés à fournir des services aériens que nous estimons être de la meilleure qualité au monde. MENZIES sert plus de la moitié des plus grandes compagnies aériennes mondiales. Ces transporteurs comptent sur nous pour travailler directement avec les passagers ainsi que dans les coulisses pour fournir des services qui font toute la différence. La gamme de services comprend des services d'escale et services aux passagers, la gestion du fret, des services d'ingénierie et l'entretien en ligne, des technologies aéroportuaires, l'exploitation des services aéronautiques d'un aéroport, un centre de formation aéronautique, une agence de voyages et le produit Pearl Assist qui inclut l'accès aux salons et les services d'accueil et d'assistance sur tout le réseau de l'entreprise. MENZIES se félicite de fournir des solutions d'aviation d'envergure mondiale.

L'entreprise est affiliée aux organismes phares de l'industrie telles que IGCH, GASA et AESA et adhèrent aux normes ISO, SGE et OHSAS. En tant que première entreprise de services d'escale du monde à obtenir la certification ISAGO, MENZIES a clairement confirmé son engagement à fournir des services d'aviation exceptionnels répondant aux normes les plus exigeantes du globe**.**

IV.3 **MISSION ET OBJECTIF**

IV.3.1 **Mission**

Par son engagement pour la qualité de service et le talent de son équipe, MENZIES met tout en œuvre pour étendre ses activités dans les marchés émergents et ainsi devenir une entreprise de gestion aéroportuaire proposant un éventail de services complet. Elle a comme mission d'assister toute compagnie aérienne aux activités Aéroportuaires.

IV.3.2 **Objectif**

La compagnie MENZIES a pour objectif de fournir les services terrestres et aériens les plus sûrs, les plus sécurisés et les plus durables, adaptés aux besoins de leur clients, et d'être ainsi reconnus comme le principal fournisseur de services aéronautiques sur le marché.

IV.4 **EMPLACEMENT GEOGRAPHIQUE**

La compagnie MENZIES se situe dans l'aéroport international de N'djili, également connu sous le nom d'aéroport international de Kinshasa, est le plus grand des quatre aéroports internationaux de la République démocratique du Congo. Nommée d'après la rivière Ndjili, elle est la principale porte d'entrée internationale vers Kinshasa et est située à 20 kilomètres (12,5 miles) au sud-est de la capitale. Il est situé dans la commune de Nsele en bordure du Malabo, à une vingtaine de kilomètres à l'est de la ville, à laquelle il est relié par le boulevard Lumumba.

IV.5 **ORGANIGRAMME**

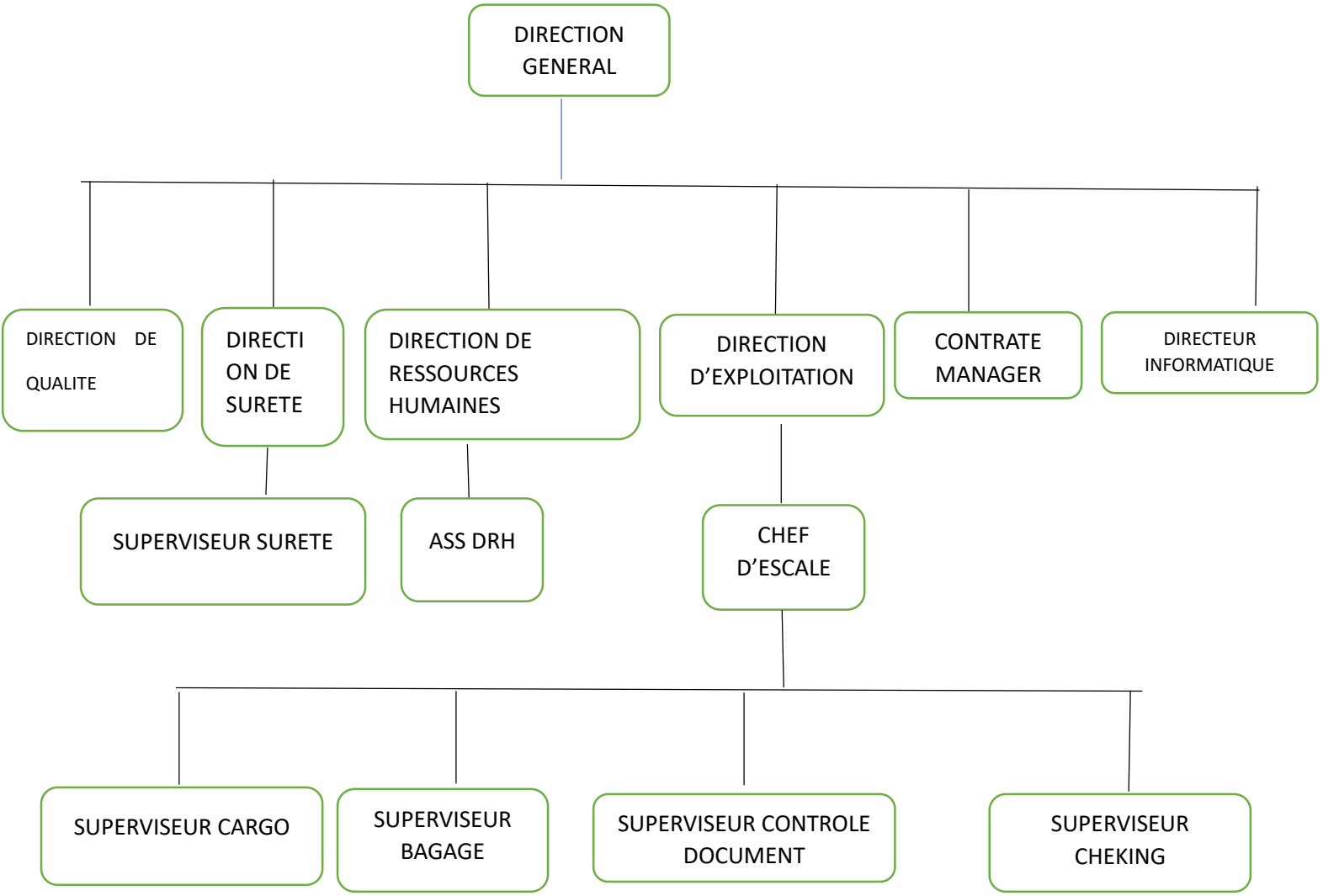


Tableau : Organigramme

IV.6 **FONCTIONNEMENT ET POSTE**

- **DIRECTION GENERAL**

La fonction Direction et Administration générale consiste à définir les objectifs, prévoir et choisir les actions à accomplir, contrôler leur réalisation, prendre d'éventuelles mesures correctives.

Il faut pour cela avoir une vision à long terme et surtout un leadership managérial avéré.

- **DIRECTION QUALITE**

La fonction Direction Qualité dirige le service qualité et propose à la direction générale toute politique concernant l'ensemble des questions de qualité des services rendus. Dans ses propositions, au-delà de la valeur ajoutée technologique ou de service clients, il doit évaluer le coût induit par les développements proposés.

Le Directeur Qualité établit et met en œuvre la démarche qualité de l'entreprise en y associant des indicateurs et des processus de contrôle. Il est responsable de la conformité des produits ou services de l'entreprise aux exigences internes et externes (conformité aux normes, exigences légales, attentes des clients…). Il coordonne les activités de pilotage et de surveillance de la performance des procédures et méthodologies qualité de l'entreprise.

- **DIRECTION SURETE**

La Politique de « Sûreté » s'intègre dans un socle commun et établit les principes généraux relatifs à la protection des personnes, des biens matériels et immatériels

Dont l'information, l'intégrité et l'image de l'Entreprise et de ses dirigeants contre toute menace malveillante, matérielle ou immatérielle.

- **DIRECTION INFORMATIQUE**

La direction informatique assure l'organisation, le suivi et la mise en œuvre de toute l'infrastructure système et informatique de l'entreprise.

- **DIRECTION D'EXPLOITATION**

Travaille au siège de la compagnie ou pour une société de handling. Il prépare le dossier de vol d'un avion en prenant les informations extérieures telles que la météorologie et la navigation aérienne. Avant chaque vol il effectue un briefing avec l'équipage. Il doit être réactif en cas d'imprévu sur le vol et pouvoir proposer au commandant de bord des solutions de déroutement. Pour cela il est en constante communication avec les autorités locales, les aéroports, l'équipage de l'avion et les équipes de l'aéroport. Il doit également se tenir informé de tous les changements de données concernant les NOTAM et les espaces aériens.

- **DIRECTION DES RESSOURSES HUMAINES**

La fonction de directeur des ressources humaines recouvre trois missions principales. Tout d'abord, la gestion du personnel. Le DRH est chargé de définir et mettre en œuvre une politique de recrutement, de promouvoir la gestion des carrières.

- **CONTRAT MANAGEMENT**

Les gestionnaires de contrats supervisent les projets réalisés en partenariat entre une organisation et une autre. Ils sont responsables de la coordination de tous les aspects du projet, de l'examen et de l'approbation des conditions contractuelles à la coordination des délais, en passant par l'approbation des budgets et plus encore

L'aéroport. Il doit également se tenir informé de tous les changements de données concernant les NOTAM et les espaces aériens.

IV.7 **SERVICE CONCERNE**

MENZIES possède trois modems Wi-Fi qui permettent à ses différents agents qui sont dans les diffèrent sites et locaux pour se connecter à l'internet et échanger des correspondances avec le reste du monde.

IV.7.1 ARCHITECTURE EXISTANTE

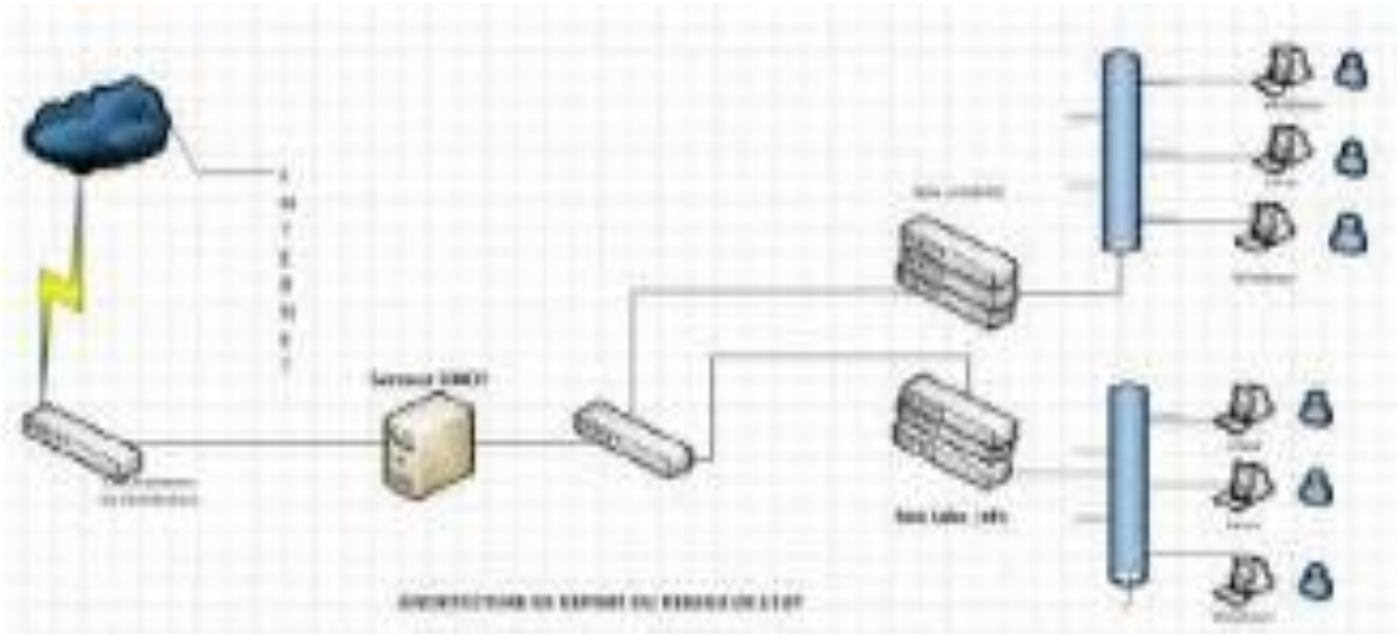


Figure 5 Architecture existante

Les attaques sur les réseaux sont des menaces croissantes et peuvent avoir des conséquences graves pour les organisations, les entreprises et même les individus. Alors que les technologies réseau se développent, les méthodes d'attaque deviennent de plus en plus sophistiquées, ce qui entraîne un besoin constant de renforcer les défenses ce qui est le cas pour la MENZIES le mécanisme de sécurité n'est pas solide.

IV.8 **CRITIQUE DE L'EXISTANT**

Les **attaques sur les réseaux** sont des menaces croissantes et peuvent avoir des conséquences graves pour les organisations, les entreprises et même les individus. Alors que les technologies réseau se développent, les méthodes d'attaque deviennent de plus en plus sophistiquées, ce qui entraîne un besoin constant de renforcer les défenses ce qui est le cas pour la MENZIES le mécanisme de sécurité n'est pas solide.

IV.9 **PROPOSITION DE SOLUTION**

Les attaques réseau peuvent avoir des conséquences catastrophiques, mais une défense en profondeur basée sur des solutions combinées de pare-feu peut considérablement réduire le risque d'intrusion.

IV.10 **CONCLUSION**

En définitive, ce chapitre sur l'étude du site, nous a permis d'avoir une vision claire sur le fonctionnement de l'entreprise, l'Etat enfin de lieux de service informatique, les équipements informatiques qu'elle dispose, ses besoins ; pour enfin définir quel système de sécurité pouvons-nous mettre en place.

Chap V **MISE EN ŒUVRE**

V.1 **INTRODUCTION**

Dans c'est chapitré nous allons mettre en place un mécanisme de sécurité pour sécuriser les attaques pour garantir le bon fonctionnement de notre système informatique.

V.2 **DEFINITION DU MECANISME DE SECURITE**

Un mécanisme de sécurité désigne un ensemble de mesures ou de dispositifs mis en place pour protéger des informations, des systèmes ou des infrastructures contre des menaces potentielles.

V.3 **TYPE DE PARE FEU**

Un pare-feu bloque les paquets de données en fonction de règles prédéfinies que vous pouvez établir. Ces outils permettent de protéger tous vos appareils, vos données et votre réseau contre les cyberattaques telles que les menaces internes, les logiciels malveillants, les attaques d'ingénierie sociale, les attaques DDoS, les menaces de type "zero-day", etc. Vous pouvez ainsi naviguer en toute sécurité sur internet.

Sur la base des techniques opérationnelles, un pare-feu peut être classé comme suit :

- Pare-feu à filtrage de paquets
- Pare-feu à inspection dynamique
- Pare-feu au niveau du circuit
- Pare-feu à proxy
- Les pare-feu de nouvelle génération (NGFW)

En fonction du modèle de livraison, ils peuvent être :

- Pare-feux logiciels
- Pare-feux matériels
- Pare-feu en nuage

D'autres types de pare-feu sont également disponibles, tels que les pare-feu basés sur l'hôte, les pare-feu UTM, les pare-feu NAT, les WAF, les pare-feu virtuels, les pare-feu de base de données, les pare-feu de conteneur, etc.

V.3.1 **SUR LA BASE DES TECHNIQUES OPERATIONNELLES**

- **Pare-feu filtrant les paquets**

Les pare-feu filtrant les paquets sont les plus anciens pare-feu capables de surveiller et de contrôler les données entrantes et sortantes lorsqu'elles circulent sur un réseau. Il crée un point de contrôle ou un filtre au niveau d'un commutateur réseau ou d'un routeur de trafic. Il filtre les données en fonction de règles prédéfinies et fonctionne au niveau du réseau.

- **Pare-feu à inspection dynamique**

Les pare-feu à inspection dynamique sont ceux qui peuvent traiter des données dynamiques et surveiller les paquets en continu sur le réseau. C'est pourquoi ils sont également appelés pare-feu à filtrage dynamique de paquets. Ils fonctionnent au niveau du réseau et de la couche de transport.

- **Passerelles au niveau du circuit**

Le pare-feu au niveau du circuit surveille et inspecte les échanges TCP dans un réseau ou d'autres activités d'ouverture de session par le biais d'un protocole réseau sur un réseau donné. Il opère dans la cinquième couche du modèle OSI (Open Systems Interconnection), appelée couche session.

- **Pare-feu proxy**

Les pare-feux proxy sont également appelés pare-feux à proxy inverse ou passerelles au niveau de l'application. Ces pare-feu fonctionnent au niveau de la couche application du modèle OSI.

- **Pare-feu de nouvelle génération (NGFW)**

Le pare-feu de nouvelle génération est un pare-feu les plus récents qui offrent une protection globale contre les menaces, qu'elles proviennent de l'intérieur ou de l'extérieur de votre réseau. Ils combinent les capacités des pare-feu traditionnels avec des systèmes et des logiciels de sécurité modernes. À l'exception de la couche physique, il fonctionne à toutes les couches.

V.3.2 **FONCTION DU MODELE DE LIVRAISON**

- **Pare-feu logiciel**

Le pare-feu logiciel est ceux que vous installez sur votre appareil local et non sur un serveur en nuage ou sur un composant matériel individuel. Ils isolent chaque point d'extrémité du réseau les uns des autres, ce qui en fait un outil efficace pour créer une sécurité approfondie.

- **Pare-feu matériel**

Le pare-feu matériel sont des dispositifs physiques qu'une organisation déploie afin de créer une frontière de réseau sécurisée ou "pare-feu". Il inspecte l'ensemble du trafic réseau entrant et sortant afin qu'aucun paquet de données nuisibles ne puisse pénétrer dans la frontière.

- **Pare-feu en nuage**

Un pare-feu en nuage est hébergé dans le nuage. Le fournisseur de services met ce type de pare-feu à la disposition des utilisateurs sous la forme d'un service par abonnement. C'est pourquoi on l'appelle aussi Firewall-as-a-Service (FWaaS).

V.4 PRESENTATION DU PARE FEU

V.4.1 PRESENTATION DE CONFIGSERVER SECURITY & FIREWALL (CSF)

ConfigServer Security & Firewall (CSF) est un outil de sécurité populaire et complet conçu pour les serveurs Linux. Il s'agit d'un pare-feu logiciel qui offre une protection contre diverses menaces réseau et qui est particulièrement utilisé dans les environnements d'hébergement, tels que les serveurs dédiés, les serveurs VPS (Virtual Private Server), ou les systèmes de gestion d'hébergement comme cPanel et WebHost Manager (WHM).

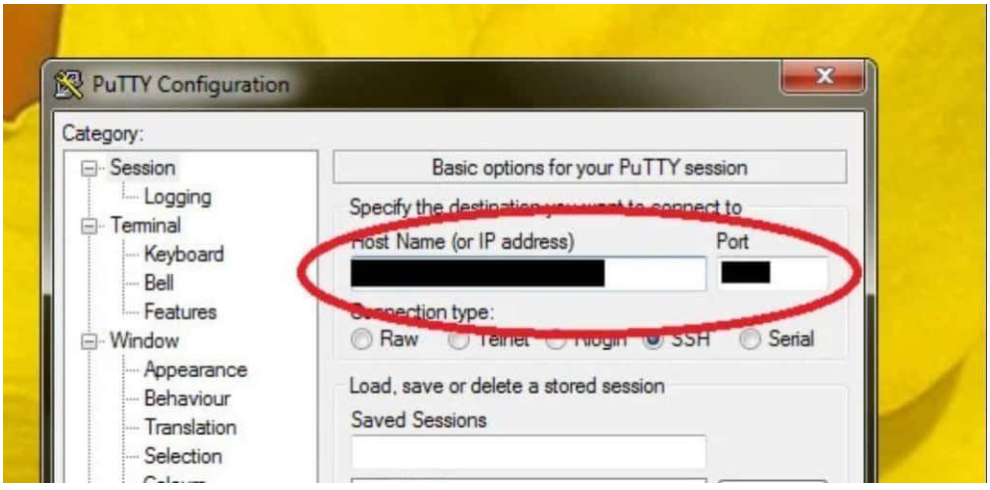
N.B : CSF est conçu pour protéger le serveur contre des attaques réseau externes (comme les attaques DDoS, les intrusions, ou les tentatives de brute force) et pour offrir une gestion simple et efficace de la sécurité réseau à travers une interface graphique facile à utiliser.

V.5 INSTALLATION DE PARE-FEU CSF

V.5.1 PREREQUIS

Pour installer et configurer ConfigServer Security & Firewall (CSF), il est essentiel d'avoir un accès root à votre serveur. L'accès root vous permet d'exécuter toutes les commandes nécessaires à l'installation et à la configuration de CSF.

Avant de commencer l'installation de CSF, assurez-vous que votre système d'exploitation et tous les paquets installés sont à jour.



Utilisez un client SSH comme PuTTY pour vous connecter à votre serveur en utilisant vos identifiants root.

Mettre à jour les paquets :

Exécutez la commande suivante pour mettre à jour tous les paquets installés :

1 yum update -y

Redémarrer le serveur (si nécessaire) :

Après les mises à jour, il peut être nécessaire de redémarrer votre serveur pour appliquer les changements. Utilisez la commande suivante :

Pour installer CSF, vous pouvez utiliser les commandes suivantes :

V.5.2 **INTSALATION DE CSF**

Pour installer CSF, vous pouvez utiliser les commandes suivantes :

V.5.3 **CONFIGURATION DU PARE-FEU**

1. **les règles de pare-feu**

Vous pouvez maintenant commencer à configurer les règles de pare-feu pour protéger votre serveur contre les attaques réseau.

A. **Configurer les ports autorisés (ports ouverts)**

Dans le fichier de configuration csf.conf, vous pouvez spécifier les ports autorisés à recevoir du trafic entrant. Utilisez SSH le port 22, HTTP sur le port 80, et HTTPS sur le port 443, vous pouvez ajuster ces règles comme suit :

Bash

Copier le code

Activer les ports essentiels

TCP_IN = "22, 80,443" Liste des ports entrants autorisés
TCP_OUT = "22, 80,443 Liste des ports sortants autorisés
UDP_IN = "53" pour DNS en entrée
UDP_OUT = "53" pour DNS en sortie

B. **Bloquer les tentatives de connexion multiples (attaque par force brute)**

Le Login Failure Daemon (LFD) intégré à CSF surveille les tentatives de connexion infructueuses et peut bloquer l'IP après un certain nombre d'échecs.

Voici quelques paramètres importants à configurer dans le fichier CSF.CONF :

Bash

Copier le code

LF_TRIGGER = "5" Nombre de tentatives échouées avant blocage
LF_SUSPEND_TIME = "3600" Durée en secondes pendant laquelle un blocage est appliqué (1 heure)
LF_EMAIL_ALERT = "1" Envoie des alertes par email lors de blocages
LF_INTERVAL = "300" Période en secondes dans laquelle les tentatives sont comptabilisées
LF_BLOCK_TIME = "3600" Durée en secondes pour laquelle une IP sera bloquée après plusieurs échecs

C. **Protéger contre les attaques DDoS (Déni de Service distribué)**

CSF permet de limiter le nombre de connexions simultanées par IP. Cela peut aider à prévenir certaines attaques DDoS de faible envergure.

bash

Copier le code
# Limiter le nombre de connexions simultanées par IP
CT_LIMIT = "20" Nombre maximal de connexions simultanées par IP
CT_INTERVAL = "60" Période (en secondes) pendant laquelle la limite s'applique

D. **Activer les protections contre les scans de ports**

Pour éviter que votre serveur ne soit ciblé par un scanner de ports, vous pouvez activer la protection contre les scans de ports.

Bash

Copier le code
PORT_SCAN_ALERT = "1" Envoie une alerte par e-mail en cas de scan de port
PORT_SCAN_IP_LIMIT = "10" Nombre d'accès (requêtes) avant de considérer comme scan
PORT_SCAN_INTERVAL = "60" Période en secondes pendant laquelle les accès sont comptabilisés

2. Configurer le Mode de blocage d'IP géographique (GeoIP)

Pour bloquer les attaques provenant de certains pays, CSF permet de configurer des règles de blocage géographique en utilisant la base de données **GeoIP**.

- Installez la base de données GeoIP :

  bash
  Copier le code

csf -g

- Dans csf.conf, vous pouvez activer la protection par pays
  bash
  Copier le code
  GEOIP_BLOCK = "1" # Active le blocage par pays

- Ajoutez les pays à bloquer dans csf.deny :

  bash
  Copier le code
  # Exemple de blocage d'un pays (Code ISO 2 lettres, par exemple 'CN' pour la Chine)
  csf -d CN

3. Utilisation des Règles de Deny/Allow Manuelles

Vous pouvez également ajouter manuellement des adresses IP à bloquer ou autoriser, directement dans les fichiers de configuration de CSF.

- Ajouter une IP à la liste noire (bloquée) :

  bash
  Copier le code
  csf -d 192.168.1.100 "Tentatives d'attaque"

- Ajouter une IP à la liste blanche (autorisée) :

  bash
  Copier le code
  csf -a 192.168.1.100 "IP autorisée"

4. Surveillance et alertes

CSF envoie des alertes par e-mail lorsque certaines actions sont entreprises (par exemple, blocage d'IP, attaque détectée, etc.). Assurez-vous que les notifications par e-mail sont configurées correctement dans le fichier csf.conf :

Bash
Copier le code
LF_ALERT_TO = "votre-email@example.com" Adresse e-mail pour recevoir les alertes

5. Vérification de la configuration

Une fois la configuration terminée, vous pouvez tester si CSF fonctionne correctement :

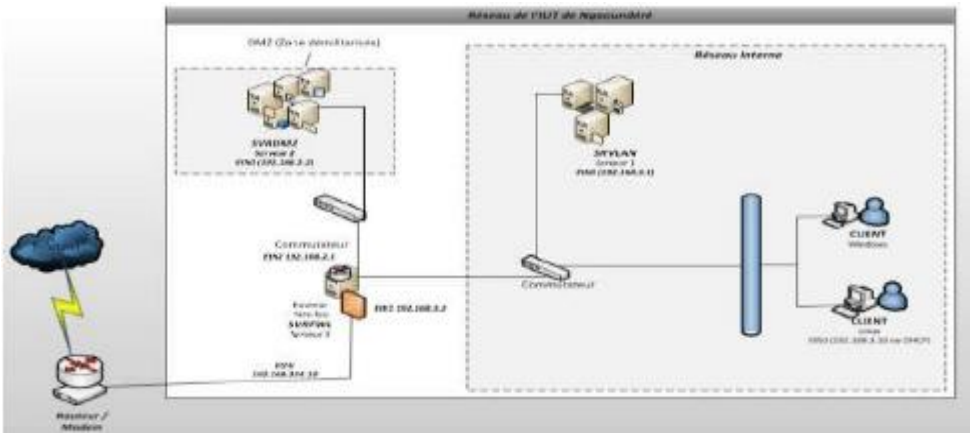
Bash
Copier le code
Vérifier le statut de CSF
csf -l # Liste les règles de pare-feu actives

csf -t # Tester la configuration de sécurité du pare-feu

V.6 **FONCTIONNEMENT DU CSF**

Le pare-feu joue un rôle crucial dans la sécurité des systèmes et des réseaux en contrôlant le trafic entrant et sortant en fonction de règles de filtrage. En filtrant les connexions suspectes ou non autorisées, il protège contre les intrusions, les attaques par déni de service, les infections par des malwares et d'autres menaces.

V.7 **ARCHITECTURE**



V.8 **AVANTAGE**

CSF est un pare-feu puissant, flexible et facile à configurer qui offre de nombreux avantages pour protéger un serveur Linux contre les attaques réseau. Son intégration avec des panneaux comme cPanel, son efficacité contre les attaques par force brute, ses nombreuses options de filtrage, ainsi que son interface conviviale en font une solution de sécurité très prisée. Si vous gérez un serveur ou un service hébergé et souhaitez mettre en place une solution de pare-feu robuste, CSF est une excellente option.

V.9 **CONCLUSION**

La mise en œuvre d'un pare-feu CSF est un moyen efficace de renforcer la sécurité d'un serveur Linux. En combinant une protection contre les attaques réseau courantes, une gestion facile via une interface web ou en ligne de commande, et une surveillance proactive, CSF devient un élément essentiel de toute stratégie de sécurité serveur. Avec une configuration appropriée, il permet non seulement de réduire les risques d'intrusions, mais aussi de répondre rapidement aux incidents de sécurité. Toutefois, pour maximiser ses avantages, une surveillance continue et des ajustements réguliers sont nécessaires pour s'assurer que le pare-feu reste performant et adapté aux besoins du serveur.

9. CONCLUSION GENERAL

Les attaques informatiques représentent un défi constant et croissant dans le monde numérique moderne, où l'interconnexion des systèmes, des réseaux et des appareils expose les individus, les entreprises et les organisations à des risques de plus en plus sophistiqués et variés. Qu'il s'agisse de malwares, de phishing, d'attaques par déni de service (DoS/DDoS), d'exploitation de vulnérabilités, ou de menaces internes, les attaques sont devenues une réalité incontournable dans le paysage de la cybersécurité.

Les conséquences de ces attaques peuvent être graves : perte de données sensibles, interruption des services, vols d'identifiants, espionnage industriel, ou encore dommages à la réputation des entreprises. De plus, les attaques informatiques sont souvent de plus en plus difficiles à prévenir, car elles évoluent constamment et s'adaptent aux nouvelles technologies et aux pratiques de défense.

Face à cette menace omniprésente, il est essentiel d'adopter une approche proactive et globale de la sécurité informatique. Cela inclut non seulement l'implémentation de technologies de sécurité robustes, telles que les pare-feu, les systèmes de détection d'intrusion (IDS/IPS), le cryptage, ou l'authentification multifacteur, mais aussi la formation et la sensibilisation des utilisateurs aux risques et aux bonnes pratiques de cybersécurité. Les humains restent souvent le maillon le plus vulnérable de la chaîne de sécurité, ce qui justifie l'importance d'une vigilance constante et d'une éducation continue.

De plus, face à la complexité croissante des menaces, la collaboration entre les acteurs publics et privés, ainsi que l'adoption de normes et de régulations de sécurité sont des leviers essentiels pour renforcer la résilience collective et la confiance dans les systèmes numériques. Les entreprises doivent également intégrer la cybersécurité dès la conception des systèmes et des applications (approche *security by design*) pour anticiper les vulnérabilités et réduire les risques.

En définitive, bien que les attaques informatiques constituent une menace permanente, elles ne sont pas inévitables. Grâce à une stratégie de sécurité informatique bien pensée, à la vigilance et à une culture de cybersécurité partagée, il est possible de minimiser les risques et de protéger les données et systèmes critiques. La sécurité informatique est un processus dynamique et évolutif, qui nécessite une adaptation continue aux nouvelles menaces, mais elle demeure un investissement indispensable pour garantir la sécurité et la pérennité de l'ère numérique.

BIBLIOGRAPHIQUE

1. OUVRAGES

- ITU, Optical Fibres, Cables and Systèmes, 2010, pp. 320-340
- VAN HEL VOORT, john WILEY & Sons, SONET/SDH explained in functional models, Edition dunod, 2005, pp 12-40
- Dean. T.Réseaux informatiques.Edition RYNALD GOULET 2001, pp 200-220
    - Jarray, B. Jaunard et A.Houle. Optical Wide Area Network Design. Soumis pour publication a journal of telecommunications systems JTS, August 2009.
- D. COMER, TCP/IP : Architecture, protocols, applications, 4e edition, Inter
- Editions (2001), pp 45-65;
- Stallings W. Network Security Essentials, 2nd edition, Prentice Hall, 2003.
- MATHON, P., Windows 2003 Server, les services réseaux TCP/IP, Editions ENI, 2003, p. 372.
- CHEY COBB, Sécurité réseaux pour les nuls, First Interactive, New York, 2003, p.287 -288.
- CLAUDE SERVIN, Réseaux & télécoms, Edition Dunod, Paris, 2003, 2006.

2. NOTES DE COURS

- BOPE, B., Réseau Informatique I,II,III, UWB/KIN, TM2/A, 2020-2021, inédit;
- BOPE, B., Réseau Informatique II, UWB/KIN, TM2/A, 2020-2021, inédit;
- NZINGA ,K , Système d'exploitation réseau et atelier III, ISIPA/KIN, TM3/A, 2020-2021, inédit.
- DENI BOTA MATUBA Administration réseau L2 UWB
- DENI BOTA MATUBA Telecommunica L2 UWB

3. WEBOGRAPHIE

- www.Prevention-incendie.be
- www.def-online.com
- www.olitec.com www.praver.fr
- http://www.commentcamarche.net/contents/secu/secuintro.php3
- *http://www.figer.com/publications/secu170398.html*
- http://samomoi.com/reseauxinformatiques/les_topologies_des_reseaux.php
- http://www.rederio.br/downloads/pdf/nt00700.pdf
- http://www-igm.univ-mlv.fr/~dr/XPOSE2008/802.1x/EAP.html

Table des matières