MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

-KOLEA-

ECOLE SUPERIEURE DE COMMERCE

Mémoire de fin de cycle pour l'obtention du diplôme de master en sciences commerciales et financières

Specialité: Finance d'entreprise

Théme :

Contrôle et Sécurité Des Systémes D'informations

Cas : Casnos

Elaboré par :

Ferkous Billal

Encadré par :

Dr. Akhrouf Mohamed

Lieu de stage : Didouche Mourad Victor Hugo

Periode de Stage : 25 juin 2023 _ 26 juillet 2023

Année universitaire : 2022/2023

Nous remercions Dieu Tout-Puissant qui nous a permis de mener à bien cette recherche scientifique et qui a été inspiré par la santé, le bien-être et la détermination.

Dieu merci, merci beaucoup.

Nous adressons nos sincères remerciements et notre gratitude au professeur superviseur (Dr . Akhrouf Mohamed) pour tous les conseils et informations précieuses qu'il nous a fournis et qui ont contribué à compléter le sujet de notre étude dans ses différents aspects.

Et n'oubliez pas de présenter la grande forme à tous les professeurs et professeurs respectés de l'école superieure de commerce .

Nous vous disons merci beaucoup pour tous vos efforts.

Je dédie mon diplôme à mon père et ma mère, que Dieu les protège et les garde comme un atout et une couronne sur ma tête. Ils ont attendu des années pour voir leur fils unique dans ce qu'ils rêvent de voir en lui. Je dédie mon diplôme à chaque ami et compagnon dans mes différentes étapes d'éducation. Nous avons beaucoup appris d'eux, non seulement avec des connaissances, mais avec la morale, l'amour, la tolérance, le dévouement et le sérieux, et à travers eux, nous avons vu la vie sous un autre angle. Ils sont vraiment une bougie pour nous à bien des égards pour nos vies.

Table des matières

Liste des abréviation

SP	**Systéme de pilotage**
SO	**Systéme operant**
SI	**Systéme d'information**
SGBD	**Systéme de gestion de base de données**
PAN	**Personnel area network**
LAN	**Local area network**
MAN	**Metropolitain area network**
WAN	**Wilde area network**
OSI	**Open systéme intercoonection**
TCP	**Transmission control protocol**
IP	**Internet protocol**
ARP	**Adresse resolution protocol**
ICMP	**Internet controle message protocol**
TCP	**Transport control protocol**
UDP	**User datagram protocol**
FTP	**File transfert protocol**
SMTP	**Simple mail transport protocol**
RPC	**Remote procedure call**
NFS	**Network file system**
RSE	**Reverse social engineering**
VPN	**Virtual private networking**
SDCM	**Sous direction de controle médical**
CRTI	**Centre de traitement informatique**
SDRC	**Sous direction de recouvrement et contentieux**
SDP	**Sous direction de prestations**
SNMG	**Saliare nationale minimum garanti**
SSi	**Securité des systémes d'informations**

Liste des figures

Résumé

Le thème du contrôle et de la sécurité des systèmes d'information est essentiel dans le domaine de la technologie de l'information et de la gestion des entreprises. Il englobe un large éventail de pratiques, de politiques et de technologies visant à protéger les données, les ressources et les processus informatiques contre les menaces potentielles, qu'elles soient internes ou externes. Voici un résumé des principaux points à retenir concernant ce thème :

- **Objectif principal** : Le contrôle et la sécurité des systèmes d'information visent à garantir la confidentialité, l'intégrité, la disponibilité et l'authenticité des données et des systèmes informatiques au sein d'une organisation.
- **Confidentialité** : Cela implique de s'assurer que seules les personnes autorisées ont accès aux informations sensibles. Des mesures telles que le chiffrement des données et la gestion des identités sont utilisées pour garantir la confidentialité.
- **Intégrité** : Il est essentiel de garantir que les données ne sont ni modifiées ni altérées de manière non autorisée. Des contrôles de sécurité, des mécanismes de détection des intrusions et des vérifications régulières contribuent à maintenir l'intégrité des données.
- **Disponibilité** : Les systèmes informatiques doivent être opérationnels lorsque nécessaire. Cela implique la mise en place de mécanismes de redondance, de sauvegardes régulières et de plans de reprise d'activité en cas de panne ou d'incident.
- **Gestion des accès** : Les organisations doivent contrôler les droits d'accès aux données et aux systèmes pour éviter les abus ou les fuites d'informations. La gestion des privilèges et les contrôles d'accès sont des éléments clés de cette dimension.
- **Surveillance et détection des menaces** : Les systèmes de sécurité doivent être capables de surveiller en permanence les activités et de détecter les comportements suspects ou les tentatives d'intrusion. **Conformité réglementaire** : De nombreuses industries sont soumises à des réglementations strictes en matière de sécurité des données. Les entreprises doivent s'assurer de respecter ces normes et de se conformer aux lois en vigueur.
- **Sensibilisation à la sécurité** : Les employés sont souvent la première ligne de défense contre les menaces. Il est donc important de sensibiliser le personnel à la sécurité informatique et de les former aux meilleures pratiques.
- **Évolution constante** : Les menaces évoluent constamment, ce qui nécessite une adaptation permanente des stratégies de sécurité. En résumé, le contrôle et la sécurité des systèmes d'information sont essentiels pour protéger les actifs informatiques d'une organisation, maintenir la confiance des clients et respecter les réglementations. C'est un domaine en constante évolution qui exige une approche proactive pour faire face aux menaces en constante mutation.

Abstract

La sécurité et le contrôle des systèmes d'information représentent un pilier fondamental de la gestion des technologies de l'information dans les organisations modernes. Cette discipline vise à préserver la confidentialité, l'intégrité, la disponibilité et l'authenticité des données et des processus informatiques. Pour y parvenir, elle met en œuvre une gamme diversifiée de mesures telles que la gestion des accès, le chiffrement, la surveillance des menaces, la conformité réglementaire et la sensibilisation à la sécurité. Dans un environnement en constante évolution, la sécurité des systèmes d'information reste un défi continu, exigeant une vigilance constante, une adaptation aux nouvelles menaces et une collaboration étroite entre les équipes techniques et les parties prenantes de l'entreprise. Ce résumé explore les principaux aspects de la sécurité et du contrôle des systèmes d'information, soulignant leur importance dans la protection des actifs informatiques et la préservation de la confiance des utilisateurs et des clients.

Cet abstract résume brièvement les points clés liés à la sécurité et au contrôle des systèmes d'information, en mettant en évidence leur pertinence et leur complexité dans le contexte de la gestion informatique moderne.

- **Mot clés :** Cybermenaces , Authentification multifactorielle , Gestion des droits d'accès , Conformité églementaire , Veille technologique , Sensibilisation à la sécurité .

Introduction Générale

Introduction General

Pour des soucis d'efficacité et de rentabilité, une entreprise communique aujourd'hui avec ses filiales, ses partenaires et va jusqu'à offrir des services aux particuliers, ce qui induit une ouverture massive à l'information.

Cette entreprise possède certaines informations qui ne doivent être divulguées ni modifiées qu'à un certain nombre de personnes ou encore qui doivent être disponibles de manière transparente à l'utilisateur.

Ces informations feront l'objet d'un détournement si le système abritant ces informations est vulnérable. La sécurité devient alors un facteur décisif du bon fonctionnement de l'entreprise si celle-ci est connectée aux réseaux.

Le principe des réseaux est basé sur celui de l'autoroute : tout le monde y a accès et c'est à chacun de se protéger. L'actualité est également tournée régulièrement vers le partage des ressources Peer to Peer ou client-serveur, qui permet de mettre en relation des utilisateurs via un même réseau interne ou étendu.

L'administrateur du réseau doit prévoir en conséquence une politique de sécurité précisant la gestion des services, les droits d'accès, les services réseau disponibles, les précautions à prendre, les procédures à suivre lorsqu'une faille a été décelée dans la protection du réseau et enfin les méthodes de sauvegarde et restauration de données.

En effet, sans une politique de sécurité régulièrement mise à jour contre les menaces et les failles réseaux, un système connecté au réseau ne survit pas assez longtemps.

En même temps que l'informatique et Internet ont révolutionné nos gestes et nos habitudes, des menaces qu'il faut connaître et apprendre à gérer ont aussi fait leur apparition en parallèle:

Les virus, qui se cachent dans la messagerie ou sur des pages Internet au contenu douteux ou les spams, ces courriers électroniques indésirables qui polluent nos boites aux lettre n'en sont que quelque exemple.

Quelles sont les menaces qui pèsent réellement sur nos matériels ? Comment s'en protéger ?

Ce mémoire à donc pour objectif d'identifier les ressources sensibles qu'il faut sécuriser dans un réseau d'entreprise, les risques et menaces potentiels liés au réseau et au système d'information et les solutions qui peuvent être mises en œuvre.

Non seulement, la compréhension du fonctionnement des menaces n'est pas un acte de malveillance, mais c'est actuellement un besoin pour tout administrateur de réseaux (réseaux d'entreprise, réseaux informatiques, réseaux de télécommunication……) qui côtoie le monde des ordinateurs, car il aura un jour ou l'autre à les affronter.

A travers cette interrogation, des questions secondaires peuvent se formuler comme suit :

- Quelles sont les menaces les plus courantes auxquelles les systèmes d'information sont exposés aujourd'hui ?
- Comment évaluer les vulnérabilités potentielles des systèmes d'information d'une organisation ?
- Quelles sont les meilleures pratiques pour élaborer une politique de sécurité des systèmes d'information efficace ?

- **Hypothèse 01** : En mettant en œuvre des technologies de détection avancées, les organisations peuvent réduire de manière significative le temps nécessaire pour détecter et répondre aux incidents de sécurité.

- **Hypothèse 02** : La collaboration entre les entreprises, les organismes gouvernementaux et les organismes de sécurité privés est essentielle pour lutter efficacement contre les menaces cybernétiques avancées.

- **Hypothèse 03** : Les systèmes d'information basés sur l'Internet des objets (IoT) présentent des vulnérabilités uniques en raison de la multiplication des points d'entrée potentiels, ce qui nécessite une sécurité spécifique.

Afin d'apporter des éléments de réponse à notre problématique, nous avons effectué une recherche documentaire approfondie ainsi qu'une enquête sur terrain afin de vérifier nos hypothèses.

Notre plan de travail se présente comme suit :

- **Le premier chapitre :** intitulé sur les concepts des systèmes d'informations ; Le système d'information (SI) est un élément central d'une entreprise ou d'une organisation. Il permet aux différents acteurs de véhiculer des informations et de communiquer grâce à un ensemble de ressources matérielles, humaines et logicielles.

- **Le deuxième chapitre** : intitulé sur les Généralités sur la sécurité des systèmes d'informations et des réseaux. Il compose de trois sections : la première section présentera La notion de sécurité informatique et Les ressources sensibles avec les composantes du cette dernière, dans la deuxième section on parlera sur les risques et vulnérabilités liés aux réseaux par la suite on traitera particulièrement les virus , et pour la troisiéme section on parlera sur les rosque qui peut menacerait la confidentialité des informations stockées .

- **Le troisième chapitre** : aura consacré pour notre étude pratique : la première section présentera l'entreprise d'accueil, la deuxième traitera le déroulement de l'enquête enfin, dans la dernière section on présentera les résultats de l'étude.

Objectifs de mémoire :

L'objectif général de ce mémoire est varier en fonction des besoins académiques, des intérêts personnels et des objectifs professionnels. Cependant, voici quelques objectifs spécifiques de cette étude sont les suivants :

- **Analyser les enjeux de sécurité actuels :** L'objectif principal de votre mémoire pourrait être d'analyser en profondeur les défis et les menaces de sécurité auxquels sont confrontés les systèmes d'information modernes.
- **Évaluer les technologies et les solutions de sécurité :** Vous pourriez vous concentrer sur l'évaluation des technologies de sécurité émergentes, telles que l'intelligence artificielle, la blockchain, ou les systèmes de détection des intrusions, et leur efficacité dans la protection des systèmes d'information.
- **Examiner les meilleures pratiques en matière de cybersécurité :** Vous pourriez avoir pour objectif d'identifier et d'expliquer les meilleures pratiques en matière de sécurité informatique, y compris la mise en place de politiques de sécurité, la formation des employés et la gestion des incidents.
- **Analyser les réglementations en vigueur :** Si vous vous intéressez à la conformité réglementaire, votre mémoire pourrait se concentrer sur l'analyse des lois et des réglementations en matière de protection des données et de sécurité de l'information, telles que le RGPD en Europe ou le HIPAA aux États-Unis.
- **Étudier les implications de la sécurité dans des secteurs spécifiques :** Vous pourriez choisir de vous concentrer sur un secteur spécifique, comme la santé, les finances ou l'énergie, pour examiner les défis et les solutions de sécurité qui lui sont propres.

Méthodologie de recherche :

cette méthodologie est pour objectif de tester les hypothèses suscitées donc on utilisera deux méthodes :

La méthode descriptive : Lorsqu'on parle d'informatisation, les systèmes d'information sont incontournables. Il est normal que dans une filière qui concerne l'informatisation, les systèmes d'informations soient largement étudiés. Étant donné l'importance du sujet .

La méthode analytique : ou bien « pratique » qui se repose sur la collection des informations dans l'entreprise casnos après avoir traité ses données pour qu'on puisse savoir sa démarche en leur systéme d'information .

Chapitre 1 :
Concept des systèmes D'informations

Introduction

Ces dernières années ont été caractérisée par l'évolution rapide des technologies de l'information et de la communication en général et de l'informatique en particulier. Les effets positifs de cette évolution ont touché touts les domaines de notre vie quotidienne et ont provoqué un changement dans notre façon de communiquer. Ce chapitre aura pour objectif de présenter quelques notions sur les systèmes d'information en premier lieu puis donnera un aperçu sur les réseaux informatiques et terminera par la notion client/serveur.

1 Les systèmes d'information :

1.1 Définition d'un système :

Un système est un ensemble d'éléments matériels ou immatériels (homme, machine, méthodes, règles) en interaction, transformant par un processus des éléments (les entrées), en d'autre éléments (les sorties). C'est donc un tout constitué d'éléments unis par des relations. Ces éléments et ces relations étant munis de propriétés.

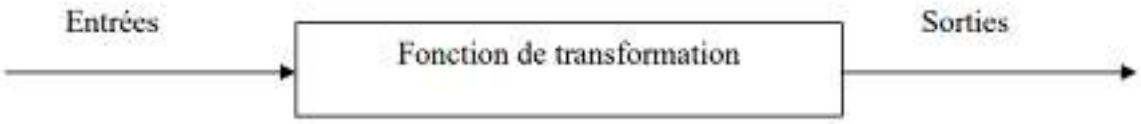

Figure 1 : Fonctionnements d'un système

Comme tout système, l'entreprise est un système :

• Ouvert sur l'environnement

• Il est finalisé (but = profit…)

• Il est en constante évolution

1.2 Système de l'entreprise : [1]

L'entreprise est composée d'un ensemble d'éléments en fonction d'un but (produit, vente…) et en interaction dynamique les uns avec les autres et avec l'environnement externe.
L'entreprise peut se décomposer en 3 sous-systèmes :

- Le système de décision (pilotage)
- Le système d'information
- Le système opérant

[1] Contribution des systèmes d'information à la performance des organisations

✓ Système de pilotage (SP) :

C'est le système nerveux de l'entreprise, car c'est lui qui prend les décisions, fixe les objectifs et les moyens pour les atteindre.

✓ Système opérant (SO) :

C'est la partie essentielle de l'entreprise, car c'est l'élément qui réalise toutes les tâches d'exploitation.

✓ Système d'information (SI) :

C'est la partie du système qui traite l'information et la véhicule entre le système de pilotage et le système opérant .

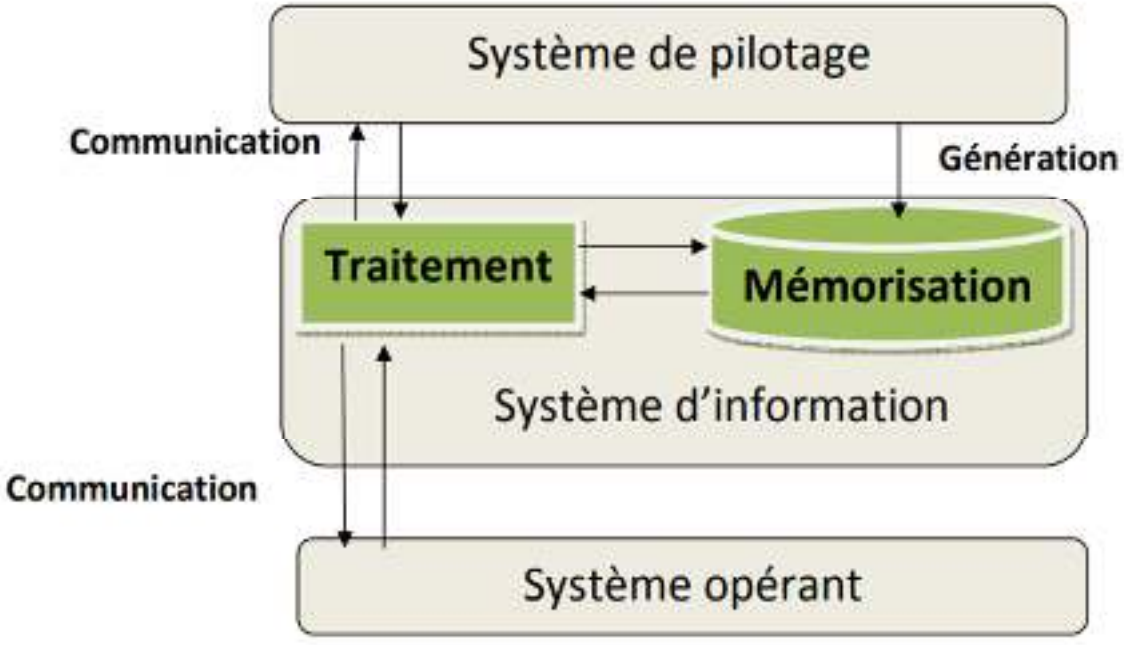

Figure 2 L'interface entre les trois systèmes

1.3 Système d'information et l'entreprise :

Un système d'information est l'ensemble des ressources (matériels, logiciels, données, procédures, ...) structurés pour acquérir, traiter, mémoriser, transmettre et rendre disponible l'information (sous forme de données, textes, sons, images, …) dans et entre les organisations.

Un système d'information est le véhicule de la communication dans l'entreprise (ou l'organisation), cette communication possède un langage dans les mots sont les données.

1.4 Fonctions des systèmes d'information dans l'entreprise : [2]

1.4.1 Recueil de l'information :

Pour fonctionner, le système doit être alimenté par des informations qui proviennent de différentes sources internes ou externes.

- **Les sources externes**

C'est l'environnement du système, il s'agit généralement des flux en prévenance de partenaire (client, fournisseur, administration,…) de plus, l'organisation doit être à l'écoute de son environnement pour anticiper les changements et adapter son fonctionnement.

- **Les sources internes**

Le système d'information doit être alimenté par des flux générés par les différents acteurs du système. La plupart de ces flux sont formalisés par des procédures, mais il existe d'autres flux d'information informelle qui sont difficiles à exploiter, mais qui ont beaucoup d'importance.

1.4.2 Mémorisation de l'information :

Les informations stockées dans les ordinateurs sont sous forme de fichiers organisés afin d'être plus facilement exploitables sous la forme d'une base de données. Le système de gestion de la base de données(SGBD) est donc une composante fondamentale d'un système d'information.

[2] https://www.syloe.com/glossaire/systeme-dinformation/#:~:text=Les%20fonctions%20d'un%20syst%C3%A8me%20d'information&text=Collecter%20%3A%20c'est%20%C3%A0%20partir,syst%C3%A8me%20d'information%20la%20conserve.

1.4.3 Traitement de l'information :

Pour être exploitable, l'information subit des traitements, là encore les traitements peuvent être manuels ou automatiques. Les principaux types de traitement consistent à rechercher et à extraire, modifier, supprimer des informations.

1.4.4 Diffusion de l'information :

Pour être exploitée, l'information doit parvenir dans les meilleurs délais à son destinataire. Les moyen de diffusion sont : support papier (courrier, note interne), forme orale et support numérique qui garantit la vitesse de transmission optimale et la possibilité de toucher un maximum d'interlocuteurs. Ceci est d'autant plus vrai à l'heure d'internet et de l'interconnexion des systèmes d'information.

1.5 Rôles d'un système d'information :

Un système d'information est :

- Un outil de communication entre le système de pilotage et le système opérant.
- Un outil de communication entre l'organisation et son environnement.
- Mettre les informations à la disposition du système de pilotage.

1.6 Qualités de système d'information : [3]

✓ **Rapidité** et **facilité** d'accès à l'information

- Trop lent ou compliqué peut décourager les utilisateurs
- L'utilisateur doit pouvoir réagir au plus vite
- Efficacité et pertinence des décisions

✓ **Fiabilité** des informations

- Informations sûres et fiables .
- Le SI doit fournir des informations à jour .

✓ **Intégrité** des informations

- Le système maintient les informations dans un état cohérent
- Le SI doit savoir réagir à des situations qui risquent de rendre les informations incohérentes

[3] guillaumeriviere.name/estia/si/pub/SI_COURS-01_2012_Introduction.pdf

- ✓ **Pertinence** de l'informatio
- Filtrer l'information en fonction de l'utilisateu
- ✓ **Sécurité** de l'informati
- Sauvegarde : si le système est critique.
- Malveillance, attaques extérieures : Routeurs filtrants, anti-virus, pare-feu…
- ✓ **Confidentialité** de l'information
- Aspect crucial, espionnage industriel, …
- Moyens matériels : Lecteurs de cartes, de badges, Lecteurs d'empreintes.
- Moyens logiciels : Identification, cryptage des canaux de transmission.

1.7 Objectifs de l'étude d'un système d'information :

L'étude d'un système d'information permet de déceler les anomalies rencontrées dans le système d'information existant, puis de proposer des solutions permettant d'une part de déterminer les dysfonctionnements actuels et d'autre part d'apporter des améliorations pour rendre son fonctionnement meilleur, st cela en tenant compte des besoins des utilisateurs.

1.8 Conception d'un système d'information :

C'est le domaine de l'information de gestion. Elle permet d'analyser et de modéliser les données et les traitements d'un domaine de l'entreprise afin de pouvoir automatiser, partiellement ou totalement, les procédures de gestion.

1.9 Méthodes de conception et de développement des SI : [4]

Une méthode est un ensemble de démarches raisonnées, suivies pour parvenir à un but. Une méthode de conception de système d'information présente une démarche et un ensemble de modèles permettant de définir et de mettre en place un nouveau système.

2 Section 2 : Les Réseaux informatiques :

[4] MethodesConception.pdf

2.1 Définition d'un réseau :

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.

Un réseau informatique est un ensemble d'ordinateurs ou terminaux qui sont reliés entre eux, capables de s'échanger des données et de partager des ressources via un réseau de transmission. Il existe deux types de réseaux :

• Les réseaux filaires composés de câbles par lesquels transitent les données ;

• Les réseaux sans fils échangeant des informations grâce à des ondes.

2.2 Classification des réseaux :

Suivant le diamètre de réseau, c'est-à-dire selon la distance maximal entre les nœuds, on peut les ranger dans une des catégories suivantes, classés par ordre de taille géographique.

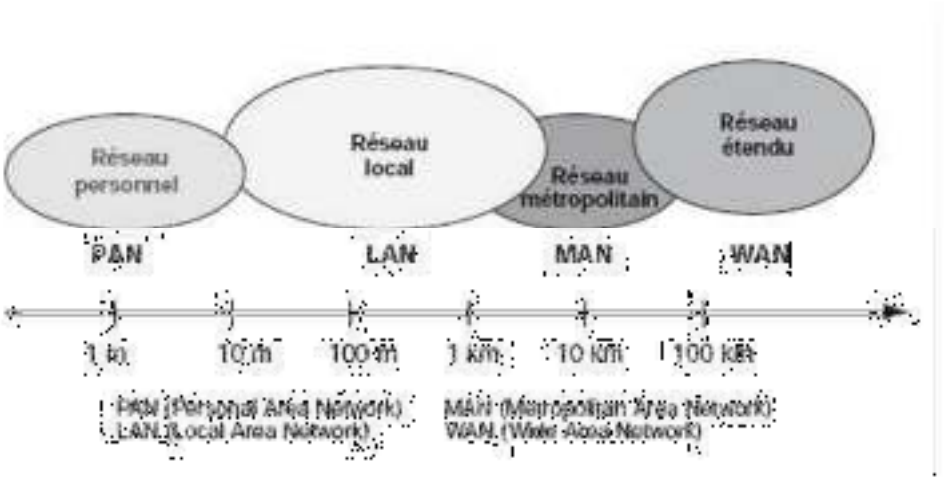

Figure 3 : Les grandes catégories de réseaux informatiques

2.2.1 Les réseaux personnels ou PAN (Personale Area Network) :[5]

Les équipements sont interconnectés par une distance très courte, voire sur quelques mètres, tels que des terminaux GSM, portables, organiseurs, … etc.

[5] "Personal Area Networks: Performance, Connectivity, and Security with IEEE 802.15.4 and ZigBee" Diego Dujovne, Guillermo Baez, Jorge M. Finochietto

Figure 4 : Réseau personnel

2.2.2 Réseau local (LAN: Local Area Network):

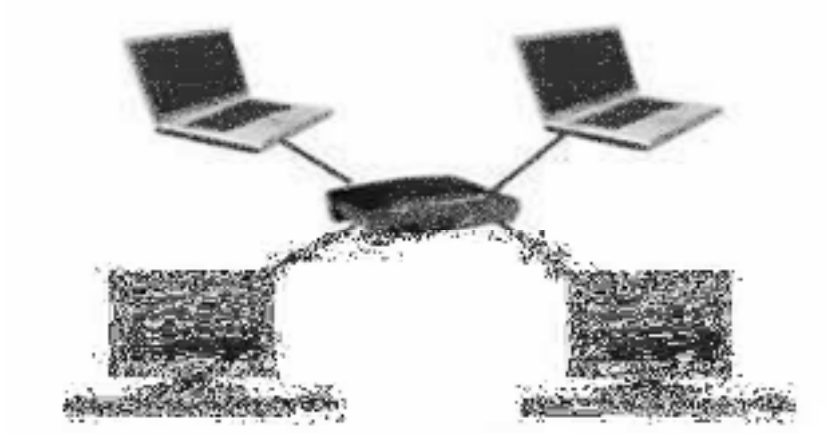

Figure 5 Réseau local

2.2.3 Réseau métropolitain (metropolitain Area Network) :

Les MAN interconnectent plusieurs LAN géographiquement proche (au maximum quelques dizaine de Km) à des débits important. Il sert généralement à interconnecter des réseaux locaux de plusieurs kilomètres. Le WMAN (Wireless MAN), également connu sous le sigle BLR (Boucle locale radio), définit un moyen de communication entre une entreprise ou un particulier et un opérateur .

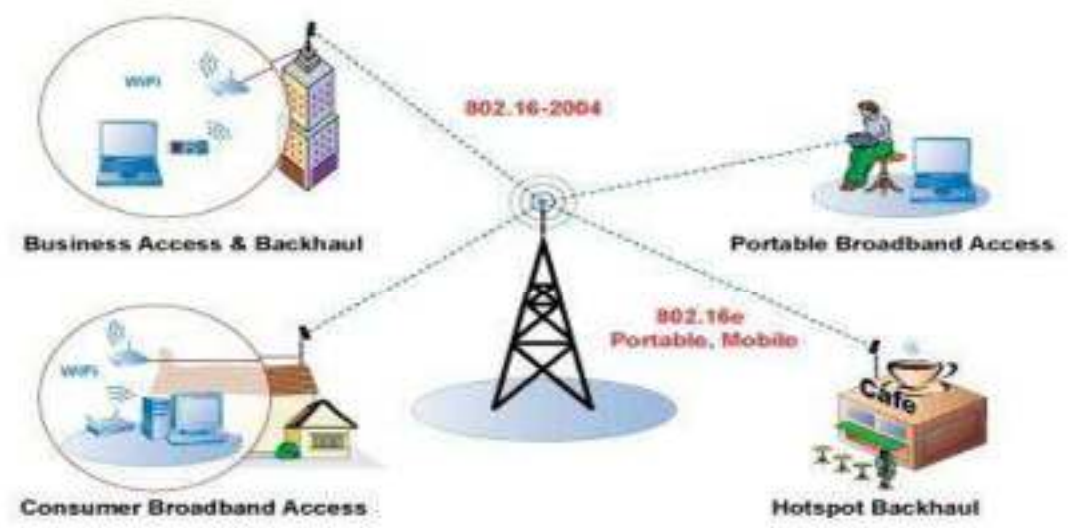

Figure 6 : Réseau Métropolitain

2.2.4 Réseau étendu (WAN: Wilde Area Network):

Le WAN appelé également réseau des réseaux, peut couvrir un pays, un continent, voire toute la planète. Il offre des moyens de communication entre des ordinateurs très éloignés. Le plus important dans le monde est : Internet. Des sociétés déploient des réseaux WiFi, appelés hosts post, connectés à Internet par une connexion ADSL ou satellitaire.

Figure 7 : Réseau WAN

2.2.5 Réseau ad hoc :

Ces réseaux sont caractérisés par le fait que chaque ordinateur le constituent est luimême un équipement de communication (Routeur) du réseau en plus d'être un Hôte .Ces ordinateurs, en tant que Routeur, sont équipés d'antennes leurs permettant d'effectuer des liaisons radio avec tous les ordinateurs situés dans leur voisinage, formant ainsi un réseau sans fils .De plus ces ordinateurs sont mobiles, ce qui induit une structure dynamique des réseaux entièrement sans fils et mobiles.

Figure 8 : Réseau Ad Hoc

2.3 Topologies de réseaux: [6]

La topologie des réseaux désigne son architecture ou la manière dont les différents équipements (ordinateurs, câblage, etc.) sont disposés et reliés entre eux. Il existe trois topologies fondamentales : en bus, en étoile, et en anneau.

2.3.1 En bus :

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans cette topologie tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câbles, généralement coaxiaux. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

Les informations envoyées à partir d'une station sont transmises sur l'ensemble du bus à toutes les stations. L'information circulant sur le réseau contient son adresse de destination et c'est aux stations de reconnaître les informations qui leur sont destinées.

On distingue deux types de topologie en bus :

- UNIDIRECTIONNEL (2 câbles distincts ou 2 canaux multiplexés),

- BIDIRECTIONNEL(Les données circulent dans les 2 sens mais non simultanément).

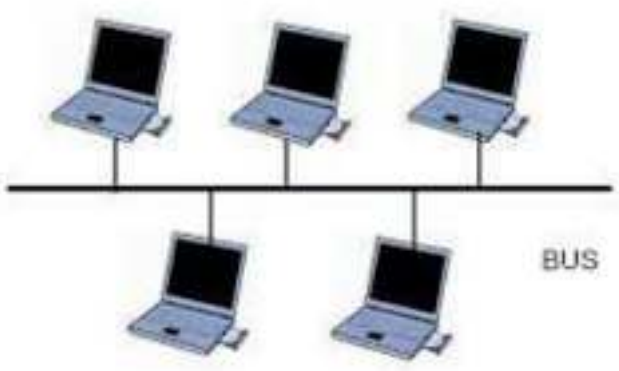

Figure 9 réseau en bus.

[6] "Computer Networking: Principles, Protocols and Practice"
Auteur : Olivier Bonaventure

2.3.2 En étoile :

La topologie en étoile des réseaux locaux est analogue à celle des systèmes centralisés à terminaux passifs : tous les nœuds sont directement reliés à un équipement central, appelé concentrateur ou hub, par lequel passent tous les messages.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux en étoile sont beaucoup moins vulnérables car on peut aisément retirer une des connexions sans pour autant paralyser le reste du réseau.

Figure 10 : réseau en étoile

2.3.3 En anneau :

C'est en fait une topologie de type bus, mais en circuit fermé, on a donc une boucle de machines sur laquelle chacune d'entre elles va communiquer à son tour. La circulation des informations s'effectue en sens unique sur la boucle ainsi constituée, ce qui élimine l'éventualité de collision entre différents messages.

Figure 11 : réseau en étoile.

2.4 Intérêt des réseaux :

Un réseau a pour but d'offrir un certain nombre de services :

- ✓ **Communication facile et rapide de l'information :** Particulièrement importante dans le domaine de la recherche qui a vu naître les grands réseaux, la communication rapide et à grande échelle de l'information est indispensable à toute organisation dont la taille dépasse le groupe d'individus.
- ✓ **Partage de ressources (matérielles, logicielles, données) :**
  - La mise en commun des ressources matérielles (imprimantes, espace disque, périphériques …) utilisées épisodiquement est une motivation à la mise en réseau.
  - La mise en commun de ressources logicielles procède de la même logique, une licence logicielle, comme une imprimante, peut être partagée. Ces deux techniques engendrent une économie de moyens.
  - La mise en commun des données est un point essentiel au bon fonctionnement d'une organisation, car la centralisation et le partage de l'information permettent d'éviter les incohérences et la duplication

Pour assurer la connexion d'une machine, il faut réunir les supports physiques. Mais pour s'assurer du bon transfert de l'information avec une qualité de service suffisante, il faut prévoir une architecture logicielle.

Une normalisation de l'architecture logicielle s'impose. Dans cette section nous allons décrire deux architectures réseau, la première provient de l'ISO et s'appelle OSI (open system interconnexion), la deuxième est l'architecture TCP/IP. [7]

2.5 Architecture OSI :

Le modèle OSI (Open Systems Interconnection ou interconnexion de systèmes ouverts) a été mis en place par l'ISO (International Standardization Organization) afin de normaliser les communications entre les ordinateurs d'un réseau. En effet, aux origines des réseaux, chaque constructeur avait un système propre (Système propriétaire) et de nombreux réseaux incompatibles coexistant, et puis le modèle OSI a autorisé de rendre la communication entre les machines standard afin que les différents constructeurs puissent mettre en œuvre des produits (logiciels ou matériels) compatibles. Le modèle OSI est un modèle qui comporte sept couches.

[7] "Computer Networks: A Systems Approach"

Larry L. Peterson et Bruce S. Davie

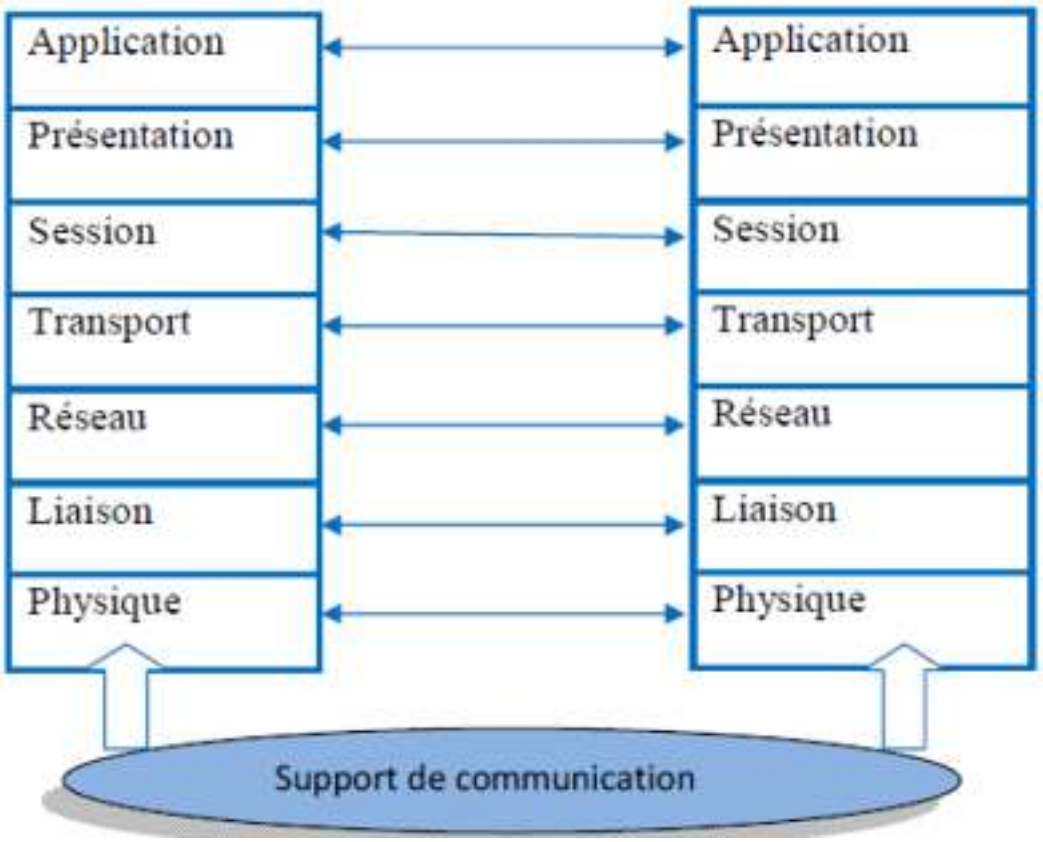

Figure 12 : hiérarchie du modèle OSI

Fonctionnalités de chaque couche :

• **Couche physique :**

Cette couche se charge essentiellement de la transmission des bits à l'état brut sur un canal de transmission de la couche 'liaison de données' à l'interface physique et vice-versa.

• **Couche liaison de donnée :**

Cette couche reçoit les données brutes de la couche physique, les organise en trames, gère les erreurs, retransmet les trames erronées, gère les acquittements (ACK) qui indiquent si les données ont bien été transmises, à la manière d'un accusé de réception. Puis, elle transmet les données formatées à la couche réseau supérieure.

• **Couche réseau :**

Son rôle est de transmettre les trames reçues de la couche 2 en trouvant un chemin vers le destinataire. Cette couche gère les sous-réseaux. Elle contrôle le trafic. Cette couche permet aussi de connecter des réseaux hétérogènes.

• **Couche de transport :**

Le rôle principal de cette couche est d'accepter les données de la couche supérieure, de les découper en paquets si nécessaire, de les transmettre à la couche réseau, et d'assurer qu'elles arrivent correctement à destination.

• **Couche session :**

Cette couche permet aux utilisateurs de machines distantes d'établir des sessions entre eux, ceci leurs permettant ainsi le transport de données. Elle permet notamment les transferts de fichiers en contrôlant et gérant les erreurs. Elle offre également l'accès à des services évolués utiles à certaines applications .

Comme le transfert de fichiers entre 2 postes. Cette couche gère la "Synchronisation". C'est à dire qu'elle insère des points de reprise dans le transfert des données de manière à ce qu'en cas de panne, l'utilisateur ne reprenne le transfert qu'au niveau du dernier point de repère.

• **Couche présentation :**

S'occupe de la syntaxe et de la sémantique des informations transportées en se chargeant notamment de la représentation des données, à savoir : Le formatage des données dans un format compréhensible par les deux systèmes. Le cryptage des données. La compression des données.

• **Couche application :**

Assure l'interface avec les applications, il s'agit donc du niveau le plus proche des utilisateurs, est géré directement par les logiciels.

2.5.1 Architecture TCP/IP :

TCP/IP désigne une architecture réseau, mais cet acronyme désigne en fait 2 protocoles Étroitement liés : un protocole de transport TCP (Transmission Control Protocol) qu'on utilise par dessus un protocole réseau IP (Internet Protocol). Ce qu'on entend par "modèle TCP/IP" c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant.

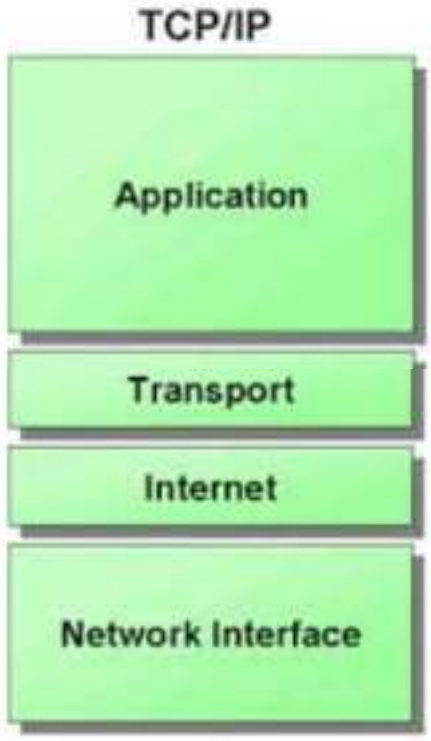

Figure 13 hiérarchie du modèle TCP/IP.

2.5.1.1 Les couche du modèle TCP/IP : [8]

a)-La couche "accès réseau" :

Elle regroupe les couches physiques et liaison de données du modèle OSI. En fait, cette couche permet à un hôte d'envoyer des paquets IP sur le réseau. Elle spécifie aussi la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé

[8] "TCP/IP Illustrated, Volume 1: The Protocols"

Auteur : W. Richard Stevens

b)-La couche internet :

La couche Internet assure la fragmentation des segments TCP en datagrammes (paquets de données) puis leurs acheminements vers des machines distantes en empruntant des chemins différents (la commutation de paquets), ainsi que de la gestion de leur assemblage à la réception.

La couche internet utilise plusieurs protocoles, les plus importants sont :

• **IP :** « Internet Protocol » gère les destinations des messages, adresse du destinataire.

• **ARP** : « Adresse Résolution Protocol » fait la correspondance de l'adresse IP (32bits) et l'adresse physique MAC (Media Access Control) de la carte réseau (48bits).

• **ICMP :** « Internet Control Message Protocol » permet d'envoyer un écho sur une station et de le recevoir.

c)-La couche transport :

Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission. La couche transport gère deux protocoles de livraison des informations, indépendamment du type de réseau emprunté :

• **TCP :** « Transport Control Protocol »assure une communication fiable on utilisant des messages d'acquittement.

• **UDP :** « User Datagram Protocole » utiliser pour des applications qui nécessitent un mécanisme de transport rapide étant donné qu'il n'intègre aucun mécanisme de contrôle de fiabilité de communication.

d)-Couche application :

La couche application est la couche située au sommet des couches de protocoles TCP/IP. Celle-ci contient des applications réseaux permettant de communiquer grâce aux couches inférieures. Il existe plusieurs protocoles et les plus répandus sont les suivant :

HTTP : ce protocole est utilisé pour la navigation web.

FTP : « File Transfert Protocol » protocole permettant d'échanger des fichiers via internet.

SMTP : « Simple Mail Transport Protocol » gestion des mails.

2.6 Correspondance entre les modèles TCP/IP et OSI :

Le modèle TCP/IP des réseaux est représenté par quatre couches protocole et découle du modèle général OSI des réseaux.

- Couche application : qui correspond à la couche application du modèle OSI.
- Couche transport : qui regroupe les couches présentation, session, et transport du modèle OSI.
- Couche accès réseau : qui regroupe la couche liaison de données et physique du modèle OSI.

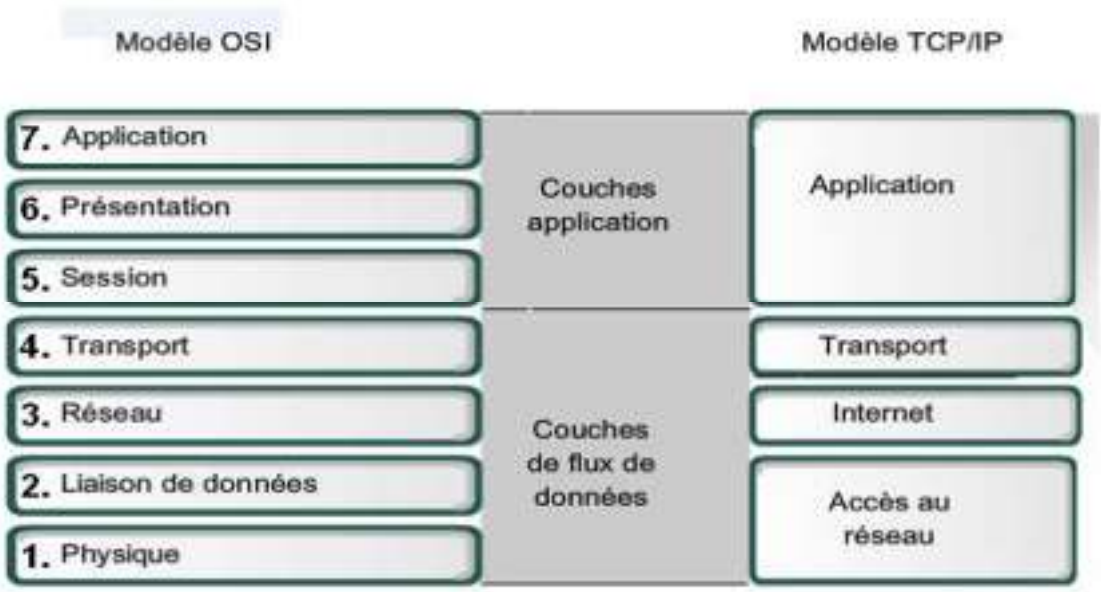

Figure 14 : correspondance entre les modèles TCP/IP et OSI

3 Section 3 : Notion client-serveur :

3.1 Introduction :

L'architecture client/serveur est apparue après un ensemble d'évolutions technologiques, qui ont été enregistrées dans les dernières années : capacité mémoire, performance des processeurs, évolution des réseaux et des différents logiciels.

Cette architecture est utilisée d'une manière très large dans plusieurs domaines. Et par conséquent les applications client/serveur sont distribuées sur plusieurs sites d'où la nécessité de les faire communiquer afin qu'elles coopèrent pour la réalisation d'un travail commun.

3.2 -Définition du Client/serveur :

C'est un modèle informatique basé sur le traitement distribué selon lequel un utilisateur lance un logiciel client à partir d'un ordinateur relié à un réseau, déclenchant simultanément le lancement d'un logiciel serveur situé dans un autre ordinateur possédant les ressources souhaitées par l'utilisateur.

3.3 -Fonctionnement d'un système client/serveur : [9]

Un système client/serveur fonctionne selon le schéma suivant:

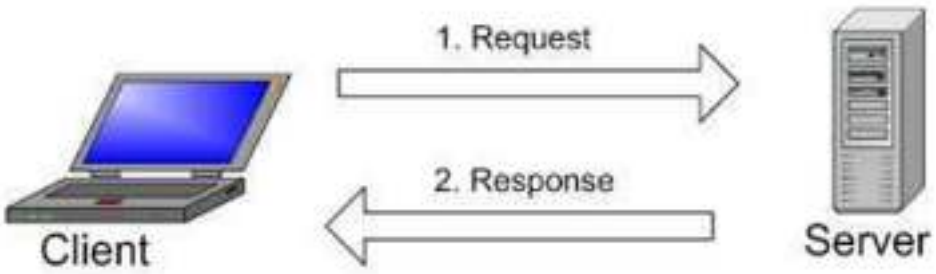

Figure 15 : Le dialogue Client/serveur

• Le client : émet une requête vers le serveur grâce à son adresse IP et le port, qui désigne un service particulier du serveur.

• Le serveur : reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port.

[9] "Distributed Systems: Principles and Paradigms"

Andrew S. Tanenbaum et Maarten van Steen

• Requête : Demande de service émise par un serveur à destination du client.

• Réponse : Message transmis par un serveur à un client suite à l'exécution d'une opération contenant les paramètres de retour de l'opération.

• Middleware (médiateur) : ensemble de logiciels construit au dessus d'un protocole de transport assurant la médiation entre le client et le serveur dans le cadre d'architecture de système hétérogène. L'objectif du médiateur est d'assurer une liaison transparente entre le client et le serveur.

3.4 Différentes architectures client /serveur :[10]

3.4.1 Architecture à 2 niveaux :

L'architecture à deux niveaux (2-tiers) caractérise le système client/serveur dans lequel le client demande une ressource au serveur qui la lui fournit directement en utilisant ses propres ressources).

Figure 16 Architecture client/serveur à 2 niveaux

3.4.2 Architecture à 3 niveaux :

Dans l'architecture à 3 niveaux (architecture 3-tiers), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :

[10] "Pattern-Oriented Software Architecture, Volume 4: A Pattern Language for Distributed Computing" Frank Buschmann, Kevlin Henney, Douglas C. Schmidt

• Un client : l'ordinateur demandeur de ressources, équipée d'une interface utilisateur (généralement un navigateur web).

• Le serveur d'application (appelé également middleware), chargé de fournir la ressource mais faisant appel à un autre serveur.

• Le serveur de données, fournissant au serveur d'application les données dont il a besoin.

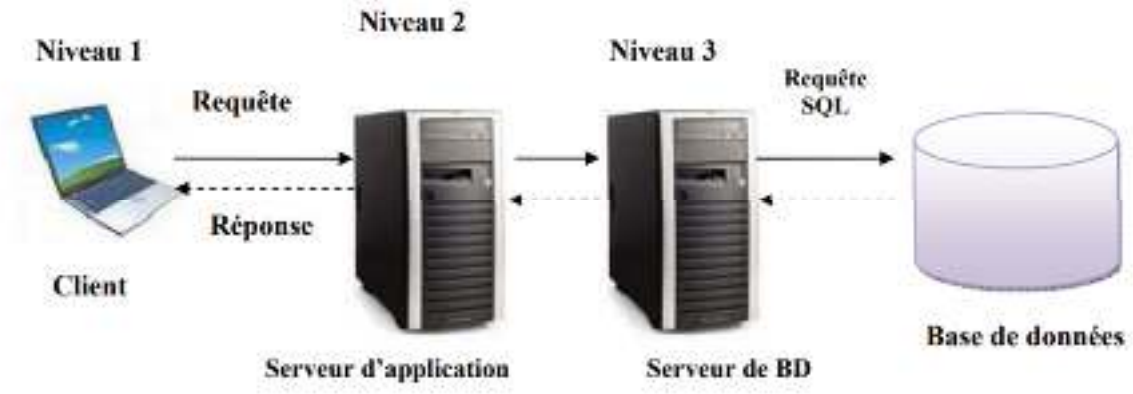

Figure 17 : architecture client/serveur à 2niveau

3.4.3 Architecture à N niveaux :

L'architecture n-tiers est la décomposition de l'architecture d'une application en plusieurs niveaux afin de découper les fonctionnalités en ensembles logiques plus facilement maitrisables. Ainsi, un serveur peut utiliser les services d'un ou plusieurs autres serveurs afin de fournir son propre service. Par conséquent, l'architecture à trois niveaux est potentiellement une architecture à N niveaux.

3.5 Les principales caractéristiques de l'architecture client/serveur: [11]

• **Hétérogénéité :** Le logiciel client/serveur est indépendant des plate formes matériels ou logiciels.

[11] "Client/Server Programming with Java and CORBA"
Robert Orfali, Dan Harkey, et Jeri Edwards

• **Souplesse et adaptabilité :** Les modifications sur le module client ne nécessitent pas des modifications sur le module serveur, la réciproque est vraie.

• **Redimensionnement :** La possibilité d'ajouter et de retirer des stations clients n'influence pas le coté serveur et la réciproque est vraie.

• **Partage des ressources :** Les clients peuvent accéder au serveur au même temps.

• **Intégrité:** les données du serveur sont gérées sur le serveur de façon centralisée. Les clients restent individuels et indépendants.

• **Localisation:** le logiciel client-serveur masque aux clients la localisation du serveur.

3.6 Avantages et inconvénients de l'architecture client/serveur :

3.6.1 Avantages :

• **Des ressources centralisées :** étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction.

• **Une meilleure sécurité :** Lors de la connexion un client ne voit que le serveur, et non les autres clients. De même, les serveurs sont en général très sécurisés contre les attaques de pirates.

• **Meilleure fiabilité :** En cas de panne, seul le serveur fait l'objet d'une réparation, et non le client.

• **Un réseau évolutif :** grâce à cette architecture il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure.

• **Une administration au niveau serveur :** l'administration se fait au niveau serveur

3.6.2 Inconvénients:

• **Un coût élevé :** la mise en place d'une architecture client/serveur nécessite un investissement important, dû aux coûts élevés du matérielles et logiciels à utiliser.

• **Un maillon faible :** le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui.

Conclusion :

Dans ce chapitre on a présenté la notion de système d'information qui permet de déceler les anomalies existantes, puis de leur proposer des solutions possibles Ensuite on a illustrée la notion des réseaux informatique qui sont des moyens pour minimiser les couts de transporte des informations et d'augmenter les performances des systèmes.

Enfin on a illustré le paradigme client/serveur, son fonctionnement et les différentes architectures possibles.

Chapitre 2 :

Généralités sur la sécurité des systèmes d'informations et des réseaux

Introduction

Pour des soucis d'efficacité et de rentabilité, une entreprise communique aujourd'hui avec ses filiales, ses partenaires et va jusqu'à offrir des services aux particuliers, ce qui induit une ouverture massive à l'information. Cette entreprise possède certaines informations qui ne doivent être divulguées ni modifiées qu'à un certain nombre de personnes ou encore qui doivent être disponibles de manière transparente à l'utilisateur.

Ces informations feront l'objet d'un détournement si le système abritant ces informations est vulnérable. La sécurité devient alors un facteur décisif du bon fonctionnement de l'entreprise si celle-ci est connectée aux réseaux.

Le principe des réseaux est basé sur celui de l'autoroute : tout le monde y a accès et c'est à chacun de se protéger. L'actualité est également tournée régulièrement vers le partage des ressources Peer to Peer ou client-serveur, qui permet de mettre en relation des utilisateurs via un même réseau interne ou étendu. L'administrateur du réseau doit prévoir en conséquence une politique de sécurité précisant la gestion des services, les droits d'accès, les services réseau disponibles, les précautions à prendre, les procédures à suivre lorsqu'une faille a été décelée dans la protection du réseau et enfin les méthodes de sauvegarde et restauration de données.

En effet, sans une politique de sécurité régulièrement mise à jour contre les menaces et les failles réseaux, un système connecté au réseau ne survit pas assez longtemps. En même temps que l'informatique et Internet ont révolutionné nos gestes et nos habitudes, des menaces qu'il faut connaître et apprendre à gérer ont aussi fait leur apparition en parallèle: Les virus, qui se cachent dans la messagerie ou sur des pages Internet au contenu douteux ou les spams, ces courriers électroniques indésirables qui polluent nos boites aux lettre n'en sont que quelque exemple.

Quelles sont les menaces qui pèsent réellement sur nos matériels ? Comment s'en protéger ?

Ce mémoire à donc pour objectif d'identifier les ressources sensibles qu'il faut sécuriser dans un réseau d'entreprise, les risques et menaces potentiels liés au réseau et au système d'information et les solutions qui peuvent être mises en œuvre. Non seulement, la compréhension du fonctionnement des menaces n'est pas un acte de malveillance, mais c'est actuellement un besoin pour tout administrateur de réseaux (réseaux d'entreprise, réseaux informatiques, réseaux de télécommunication……) qui côtoie le monde des ordinateurs, car il aura un jour ou l'autre à les affronter.

Section 1 : introduction à la sécurité des systèmes informatique

La notion de sécurité informatique couvre, en pratique, de larges problématiques.

Toutefois, s'il ne faut retenir qu'une seule définition, ce serait sans doute celle-ci : la sécurité consiste à adapter votre outil à l'organisation de votre entreprise et notamment définir qui doit avoir accès à quelles informations. Comme vos locaux, vos informations et votre réseau doivent être protégés.

La sécurité informatique, d'une manière générale doit donc assurer que les ressources sensibles d'une organisation sont disponibles et utilisées dans le cadre où il est prévu qu'elles le soient. Cela signifie que la sécurité informatique devrait être abordée dans un contexte global impliquant

- La sécurité logique, c'est-à-dire la sécurité au niveau des données ;
- La sécurité des télécommunications ;
- La sécurité des applications ;
- La sécurité physique, soit la sécurité au niveau des infrastructures matérielles.

3.7 1. Les ressources sensibles

1.1 Les ressources humaines

Ce sont paradoxalement les personnes chargées de la sécurité et de l'administration des systèmes qui représente le risque humain le plus courant susceptible d'attenter à la sécurité d'un réseau.

Parce que ces responsables ont accès à tout, et qu'ils ne sont pas à l'abri d'une simple erreur, les matériels d'un réseau et donc l'ensemble des utilisateurs, peuvent en subir les conséquences.

Par ailleurs, toute personne ayant accès à une machine court un risque, quel que soit son niveau. Son mot de passe par exemple peut fort bien tomber sous le regard d'un pirate sans scrupule et expérimenté.[12]

[12] "Gestion des Ressources Sensibles"

Claude Rocacher et Bernard Sionneau

1.2 Les ressources logicielles[13]

Aucun logiciel un tant soit peu complexe n'est exempt de « bug ». On a coutume de dire qu'un logiciel n'est jamais aussi efficace que le jour ou on n'en a plus besoin, car alors la plupart des erreurs qu'il pouvait comporter ont été corrigées. De ce fait, un logiciel peut fort bien, par erreur ouvrir une porte dans un système informatique en réseau, créant ainsi une faille de sécurité et permettre ainsi au pirate de tout ordre de s'infiltrer dans le système et de nuire à son intégrité.

1.3 Les Ressources physiques et matérielles

1.3.1 Les locaux

Un autre aspect non négligeable de la sécurité réseau est représenté par la sécurité physique. Elle constitue l'une des premières barrières à mettre en place, la sécurité d'un système réseau (informatiques, téléphoniques…) commence par celles des locaux accueillant les matériels. En effet, toute mesure de contrôle du système sera déjà fortement compromise si l'on permet à n'importe qui de pénétrer dans les locaux sensibles.

1.3.2 Les voies d'accès

La porte d'entrée n'est pas le seul moyen d'accès dans un central informatique ou télécommunication, il est, par conséquent très important de faire une liste des divers risques : une cloison ou une vitre peut se briser facilement, une gaine d'aération n'est pas forcément trop petite pour un homme, et enfin, il ne faut surtout pas oublier de protéger les câbles de connexion à des réseaux. Si, malgré tout, une intrusion malveillante est encore possible, le meilleur moyen de protection contre le vol d'un outil de télécommunication ou d'une station consiste à l'attacher à son support, ou à le fixer solidement au mur.

1.4 Les données

La protection des données se justifie en trois points bien distincts :

1.4.1 La disponibilité

On aime en générale avoir accès aux données en quasi-permanence.

1.4.2 Le secret

[13] "Gestion des Ressources Logicielles"

Auteur : Sami Beydeda, Volker Gruhn, et Uwe Assmann

La notion de secret est très importante dans certaine entreprise. Imaginer un instant que quelqu'un puisse avoir accès aux données du nouveau produit que Microsoft® veut mettre en place, il va sans dire que quel que soit le type d'entreprise le fait de savoir que les secrets de tel ou tel produit est bien gardé est quelque chose de for plaisant. Il nous viendrait à l'esprit de séparer nos données confidentielles des accès réseau, une fois cela réalisé, pourquoi se soucier de l'aspect sécuritaire et tout simplement parce que le secret n'est pas l'unique point qu'il faut prendre en compte.

1.4.3 L'intégrité

Vous devez toujours vous soucier de l'intégrité et de l'accessibilité de votre système. En effet, même si vos données ne sont pas secrètes, vous souffrirez des conséquences de leur modification ou de leur destruction.

Lorsque des données sont modifier ou détruits à votre insu, il faut dans la plupart des temps consacrer du temps à la reconstitution des dommages, ce qui bien évidemment nécessite du temps et de l'argent.

Voilà pourquoi, bien sécuriser un réseau est quelque chose de primordial. Il y a aussi un aspect qu'il faut prendre en compte, la perte de confiance de la part de vos clients, investisseurs et autres, qui, lorsqu'ils savent que vous vous êtes fait pirater ne veulent plus vous faire confiance.

1.5 La réputation

La notion de réputation est très importante, en effet, la plus part des entreprises préfèrent ne pas faire savoir que leur entreprise a été piratée tout simplement pour éviter une mauvaise publicité.

Dire qu'on a été piraté insinue que votre site n'est pas du tout sécurisé. Le pirate apparaît généralement sur Internet avec votre identité, il se sert de votre identité pour aller créer des dommages à d'autres sites. Les messages provenant d'un intrus ayant eu accès à votre site ressembleront exactement aux vôtres parce que se seront les vôtres. Inutile donc d'imaginé ce que peut être la réputation d'une entreprise ayant l'étiquette gruyère.

C'est pourquoi il faut mettre en place une bonne politique de sécurité ; mais avant de faire cela il faut déterminer contre quoi vous essayez de vous protéger.

La question est maintenant de savoir quels sont les risques et vulnérabilités qui sont omniprésents dans les systèmes réseaux ?

Section 2 : Risques et vulnérabilités liés aux réseaux [14]

Lorsqu'une organisation telle qu'une entreprise, par exemple, envisage de fonder un réseau, il faut impérativement considérer le facteur sécurité.

En effet, une connexion au réseau ne se fait pas sans risque. Un grand nombre d'utilisateurs des réseaux ne sont pas conscients des risques et des vulnérabilités liées à ces réseaux.

Ces vulnérabilités viennent surtout d'une mauvaise protection du réseau interne de l'entreprise, le niveau de sécurité du réseau interne est primordial.

On distingue plusieurs types de risques qui peuvent être regroupées en plusieurs catégories:

- Les vulnérabilités du réseau interne. L'introduction des services Internet dans un réseau d'entreprise peut ouvrir des trous de sécurité qui permettent à des intrus d'accéder au reste du réseau interne que ce soit physiquement ou logiquement.

- Les vulnérabilités des serveurs. On peut accéder à un serveur du réseau interne à partir de l'Internet pour lire ou même modifier les fichiers qu'il contient. Une société spécialisée dans la vente par correspondance (*on-line)* qui mémorise des numéros de carte de crédit sur un serveur connecté sur l'Internet est particulièrement exposée à ce risque.

- Les vulnérabilités de la transmission des données. La confidentialité et l'intégrité des informations peuvent être violées si un agresseur intercepte les communications du réseau d'entreprise (messagerie, serveur d'information, téléchargement de fichiers, etc.).

[14] "Hacking Exposed: Network Security Secrets & Solutions"

Auteurs : Stuart McClure, Joel Scambray, et George Kurtz

• Les risques de la disponibilité. Un agresseur malveillant peut réaliser une attaque qui rend des machines, ou même le réseau tout entier, indisponible pour les utilisateurs légitimes.

• Les risques de répudiation. Un partenaire dans une transaction en ligne peut nier qu'une transaction n'ait jamais eu lieu.

2.1 Les vulnérabilités techniques

2.1.1 Vulnérabilité du service TCP/IP[15]

La vulnérabilité des services TCP/IP est due au fait que beaucoup de ces services ne sont pas surs et peuvent être compromis par des intrus bien informés. Dans un environnement LAN, ce sont surtout les services visant à améliorer l'administration du réseau qui présente le plus de vulnérabilités.

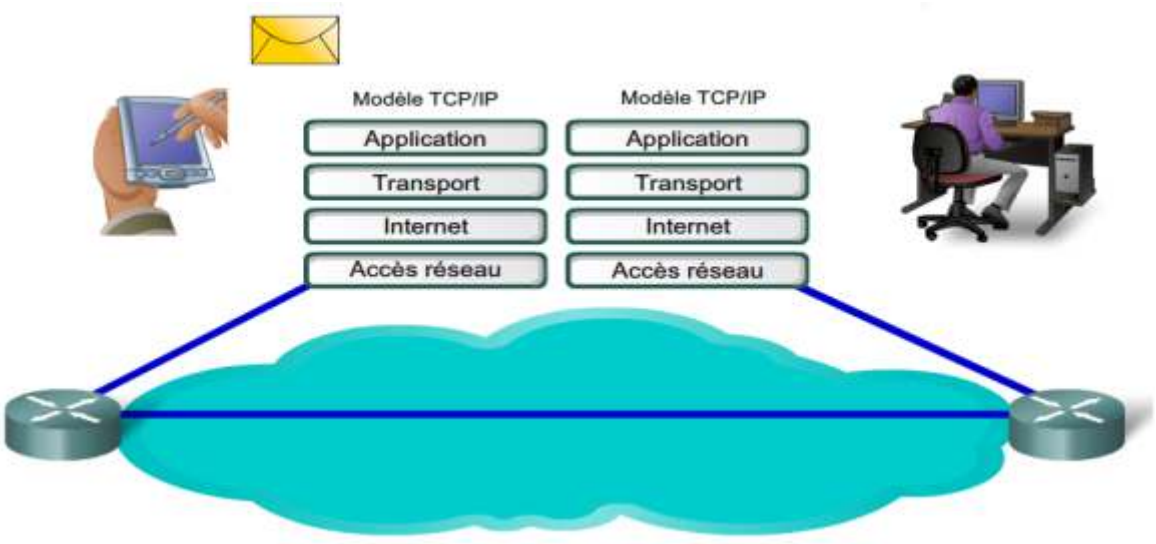

Figure 18 : Les 4 couches du protocole TCP/IP

Ces vulnérabilités hérité du manque de sécurité de TCP/IP se retrouvent dans un grand nombre d'applications comme celles basées sur les services RPC (Remote Procedure Call) comme NFS (Network File System), NIS (Network Information Service), les serveurs FTP, les serveurs de messageries notamment sendmail, etc .

[15] "Network Security Essentials: Applications and Standards"

Auteurs : William Stallings

De plus, le pilote protocolaire TCP/IP de plusieurs systèmes d'exploitations ne vérifie pas correctement certaines allocations de mémoire.

Un utilisateur malveillant peut s'appuyer sur cette vulnérabilité pour exécuter du code arbitraire à distance, ou perturber l'accès au système ciblé.

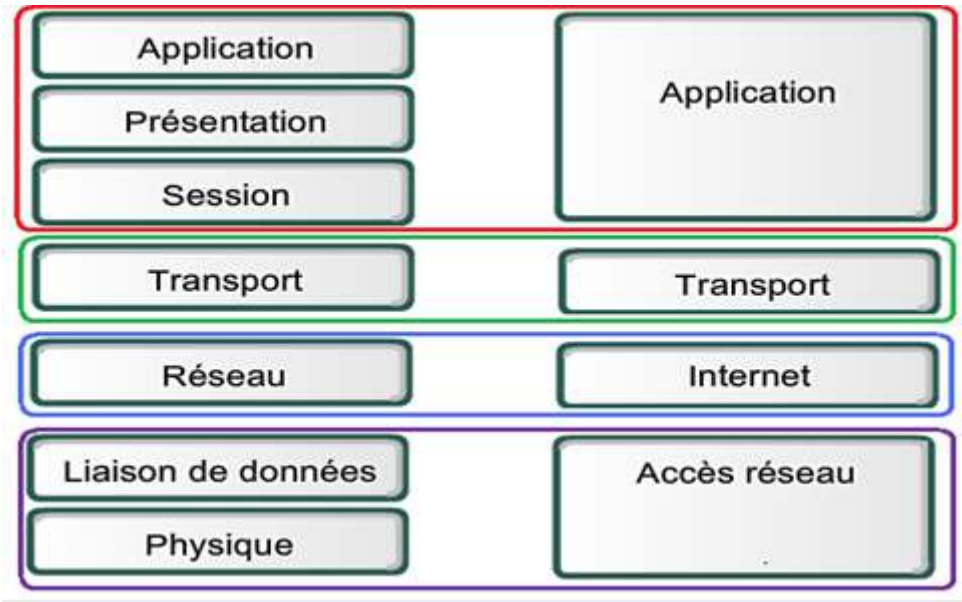

Figure 19 : Architecture réseau à 4 couches

2.1.2 Vulnérabilité des données

La facilité d'espionnage et de trucage des communications résulte du fait que la plupart du trafic qui transitent sur les réseaux, s'effectue "en clair", c'est-à-dire sans procédé de chiffrement.

Par conséquent, les lignes de communication et donc les transferts de messages électroniques (*e-mail*), de mots de passe, de fichiers peuvent être surveillé et enregistrer à l'aide de logiciels spécialisés.

2.1.3 Les vulnérabilités dues à l'absence de politique de sécurité

Il n'est pas rare de constater qu'un réseau d'entreprise, par exemple, autorise plus de services entrée/sortie que nécessaire.[16]

[16] "TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference"

Or, il est primordial de limiter l'accès à ces services qui peuvent permettre à un intrus connaissant bien le réseau interne d'obtenir des informations précieuses pour sa tâche d'espionnage ou de sabotage.

Il est donc nécessaire d'établir une politique de sécurité définissant les restrictions d'accès et d'utilisation des services à appliquer.

2.1.4 Les vulnérabilités liées aux erreurs de configuration

Le paramétrage de dispositifs de sécurité telles que des routeurs filtres permettant grâce à des listes d'accès (*access-list*) de limiter l'accès à des services, est souvent complexe et peut entraîner des erreurs de configuration accidentelles.

De telles erreurs peuvent réduire à néant l'efficacité d'une politique de sécurité.

3. Les attaques informatiques utilisant des techniques

3.1 Chevaux de Troie

La légende veut que les Grecs, n'arrivant pas à pénétrer dans les fortifications de la ville de Troie, aient l'idée de donner en cadeau un énorme cheval de bois en offrande à la ville en abandonnant le siège. [17]

Les Troyens (peuple de la ville de Troie), apprécièrent cette offrande à priori inoffensive et la ramenèrent dans les murs de la ville. Cependant le cheval était rempli de soldats cachés qui s'empressèrent d'en sortir à la tombée de la nuit, alors que la ville entière était endormie, pour ouvrir les portes de la cité et en donner l'accès au reste de l'armée

Auteur : Charles M. Kozierok

[17] "The Art of Deception: Controlling the Human Element of Security"

Auteur : Kevin D. Mitnick

Figure 20 : La fiche Cheval de Troie

Les chevaux de Troie (« Trojan horse » ou « Trojans » en anglais) tirent leur nom de cette célèbre légende mythologique. Comme cette dernière, ils utilisent une ruse pour agir de façon invisible, le plus souvent en se greffant sur un programme anodin.

Ils font parties des grandes menaces que l'on peut rencontrer sur le web, parmi les virus et autres vers. Pourtant, contrairement à ceux-ci, les chevaux de Troie ne se reproduisent pas (en tout cas, ce n'est pas leur objectif premier).

Ce sont à la base de simples programmes destinés à être exécutés à l'insu de l'utilisateur.

3.1.1 Définition

Un cheval de Troie est un programme informatique simulant de faire quelque chose, mais faisant tout autre chose à la place. A la façon du virus, le cheval de Troie est un code caché dans un programme sain qui exécute des commandes sournoises, et qui généralement donne un accès à la machine sur laquelle il exécuté en ouvrant une porte dérobée (backdoor), le Trojan s'infiltre par la suite sur le disque dur pour y effectuer des actions néfastes une fois à l'intérieur, dès qu'on exécutera son fichier porteur. Un cheval de Troie est donc conçu pour espionner et infiltrer les systèmes. Ils sont furtifs et très difficiles à détecter, surtout tant que l'attaquent ne cherche pas à se manifester. Il est évidemment utilisé par les pirates (Hackers, Crackers, Script kiddyes…) Pour prendre le contrôle d'un PC.

3.1.2 Principes

Le principe des chevaux de Troie étant d'ouvrir un port de votre machine pour permettre à un pirate d'en prendre le contrôle (par exemple voler des données personnelles stockées sur le disque), le but du pirate est dans un premier temps d'infecter votre machine en vous faisant ouvrir un fichier infecté contenant le troyen et dans un second temps d'accéder à votre machine part le port qu'il à ouvert.

Toutefois pour pouvoir s'infiltrer sur votre machine, le pirate doit généralement en connaître l'adresse IP. Ainsi

- Soit vous avez une adresse IP fixe (cas d'une entreprise ou bien parfois de particuliers connecté par câble,) auquel l'adresse IP peut être facilement récupérée .

- Soit votre adresse IP est dynamique (affectée à chaque connexion), c'est le cas pour les connexions par modem ; auquel cas le pirate doit scanner des adresses IP au hasard afin de déceler les adresses IP correspondant à des machines infectées.

3.1.3 Modes d'action

Leur mode opératoire est souvent le même; ils doivent tout d'abord être introduits dans le système cible le plus discrètement possible. Les moyens sont variés et exploitent le vaste éventail des failles de sécurité, du simple économiseur d'écran piégé (envoyé par mail ou autre, du type , , etc, etc) jusqu'à l'exploitation plus complexe d'un buffer overflow.

Après leur introduction dans le système, ils se cachent dans des répertoires système ou se lient à des exécutables. Ils modifient le système d'exploitation cible (sous Windows, la base des registres) pour pouvoir démarrer en même temps que la machine.

3.1.4 Objectif

Leur objectif est d'ouvrir une porte dérobée(« backdoor ») sur le système cible, permettant par la suite à l'attaquant de revenir à loisir épier, collecter des données, les corrompre, contrôler voir même détruire le système.

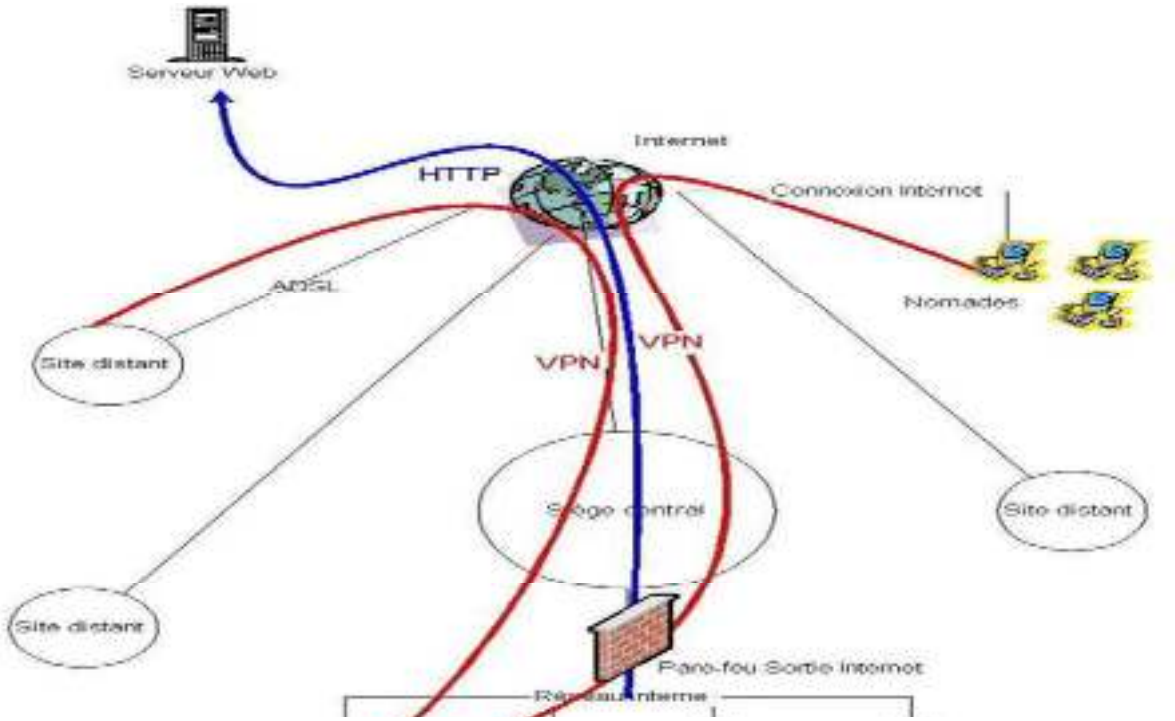

Figure 21 : VPN et Firewall

3.2 Espiogiciels[18]

A chaque connexion Internet, un utilisateur laisse derrière lui très grand nombre d'informations.

Ces traces sont généralement intéressantes mais non suffisantes à un public de professionnels ou d'espions cherchant à obtenir d'autres éléments que ces techniques laissés en standard.

[18] "Counterespionage for Corporate Professionals: How to Prevent, Detect, and Respond to Espionage Threats, Trade Secrets Theft, and Anti-Competitive Activities"

Peter W. Singer

Les professionnels d'un secteur déterminé cherchent à connaître les habitudes de téléchargement de leurs clients, leurs modes de consommations, leurs centres d'intérêts, ou la périodicité de leurs achats par exemple. Les pirates ou espions seront, eux, plus intéresse par le contenu des machines connectées, la réception de ces informations, etc

Pour faciliter la récolte de ce type de renseignements, il existe des « espiogiciels ».

3.2.1 Définition

Un espiogiciel est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé (on appelle donc parfois mouchard) afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes (profilage)

Ils se trouvent généralement dans le code d'un programme que l'utilisateur téléchargera innocemment sur Internet.

Dans la plupart des cas, ces espiogiciels sont des « petits morceaux de codes parasite » (routines) intègres dans le code principal du programme. Dans un même programme, il peut y avoir plusieurs routines parasites différents, ayant chacune une fonction déterminée.

3.2.2 Objectif

L'objectif de l'espiogiciel est simple : récolter le maximum d'information possible sur un internaute. Les récoltes d'informations peuvent ainsi être :

- La traçabilité des URL des sites visités,
- Le taquage des mots –clés saisis dans les moteurs de recherche,
- L'analyse des achats réalisés via Internet,
- Voire les informations de paiement bancaire (numéro de carte bleue / VISA) ou bien des informations personnelles.

3.2.3 Les types des Spywares

On distingue généralement deux types de spywares :

- Les spywares internes (ou spywares intégrés) comportant directement des lignes de codes dédiées aux fonctions de collectes données.
- Les spywares externes, programmes de collectes autonomes installées.

4. Keyloggers [19]

4.1 Définition

Keyloggers ou Enregistreurs de frappes sont des portion de codes très dangereux, ils ne sont pourtant pas répertoriés parmi les virus, vers, ou chevaux de Troie car n'ont pas pour objectif de modifier quoi que ce soit dans la machine cible.

Ces programmes, très furtifs, sont à l'affût de ce que vous tapez sur votre clavier, notamment des identifiants et des mots de passe.

Les Keylogger se connecte ensuite au Net et envoie les informations ainsi collectées au pirate, qui peut ainsi s'introduire dans votre système sans effort.

Figure 22 : Action du Keylogger

4.2 Objectif

L'objectif des Keylogger est d'enregistrer et de restituer tout le travail qui a été réalisé par un utilisateur.

Les touches enregistrées permettent effectivement de rétracter non seulement le travail courant, mais aussi de récupérer tous les identifiants et mots de passes.

[19] "Keylogger Developer's Guide"

Doug Huges

Certains Keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute activité de l'ordinateur!

3.8 5. Virus

En 1983, le chercheur Fred Cohen définissait un virus informatique ainsi « un programme qui peut contaminer un autre programme en le modifiant pour inclure une copie de lui-même », en d'autres mots, tous les virus se reproduisent d'eux-mêmes. Pour bien jouer le jeu, la plupart des virus tentent d'échapper aux détections, soit en utilisant des méthodes d'encryptage ou en effectuant de légères mutations chaque fois qu'ils se reproduisent.

Un virus informatique partage bien des traits communs avec son homologue biologique.

Comme lui, il ne peut survivre par lui-même : il doit s'associer intimement avec un objet du système afin d'en faire son vecteur, et le détourner pour assurer sa reproduction et, donc, sa survie. Actuellement, plusieurs virus ont une charge utile, c'est-à-dire un ensemble d'instructions conçu pour

Les virus utilisent souvent l'horloge interne de votre ordinateur pour déclencher la charge utile à une date particulière, les vendredis 13 et les anniversaires célèbres sont populaires

5.1 Principes de fonctionnement

5.1.1 Mécanisme de réplication

Ce mécanisme permet au virus de se répliquer. Il y a plusieurs méthodes pour y arriver :

- soit en infectant davantage de fichiers
- soit en utilisant un service réseau pour infecter d'autres ordinateurs

5.1.2 Charge utile

La charge utile est le coeur même du virus, c'est elle qui contient sa capacité de nuisance réelle.

Elle peut être l'une de celles-ci :

- Affichage d'un message,
- Altérations mineures de fichiers,

- Destruction du contenu d'un disque dur,
- Détérioration lente du contenu des fichiers avec ou sans possibilité de restauration,
- Vol ou diffusion d'informations confidentielles.

5.1.3 Déclencheur

Le déclencheur peut être réglé pour :

- Une action immédiate
- Une action ponctuelle (un jour particulier)
- Une action répétitive (à chaque démarrage du système)

5.2 Mécanisme de protection[20]

Compression :

La compression est faite pour limiter la taille du code du virus, pour offrir un plus petit motif pour les anti-virus et pour ne pas attirer l'attention par des pertes de taille de disque.

Polymorphisme :

Le polymorphisme permet de limiter la reconnaissance du code par les scanners anti-virus.

Furtivité :

Il s'agit ici de rendre plus difficile la détection par l'anti-virus en détournant tous les appels au disque.

Multiples phases :

C'est une méthode exotique de création de virus qui consiste à le faire passer par plusieurs modes d'infection. Le virus peut agir comme un virus macro puis comme un virus résident infectant les fichiers par des macros.

5.3 Caractéristiques

5.3.1 La résidence

[20] "Computer and Information Security Handbook"

John R. Vacca et Trevor A. Israelsen

Dès son exécution, le virus s'extrait de son hôte et va se loger dans la mémoire vive où il prend le contrôle de la machine ;

5.3.2 La cryptographie

A chaque réplication, le virus est chiffré (afin de dissimuler les instructions qui, si elles s'y trouvaient en clair, révéleraient la présence de ce virus ou pourraient indiquer la présence de code suspect);

5.4 Les catégories de virus

5.4.1 Virus de Zone d'amorce

Un virus de zone d'amorce utilise la méthode la plus simple existante pour se propager. Il infecte la zone d'amorce des disques durs et des disquettes.

Pour être infecté, il faut avoir démarré sur une disquette, ou un disque amovible contenant le virus. Une fois la zone d'amorce de l'ordinateur infectée, ce virus se transmettra sur toute disquette ou support amovible inséré dans l'ordinateur.

5.4.2 Virus DOS

La plupart des virus fonctionnent sous le système d'exploitation DOS. Il est beaucoup plus simple d'écrire un virus pour DOS, car DOS existe depuis beaucoup plus longtemps que Windows et il y a donc beaucoup plus de gens ayant l'expertise nécessaire à ce genre de pratiques. De plus un virus écrit sous DOS sera beaucoup plus petit en taille que son équivalent écrit sous Windows.

5.4.3 Virus Windows [21]

Les virus Windows fonctionnent sous Windows et vont pouvoir infecter les programmes Windows. Le nombre de virus Windows est beaucoup plus réduit que le nombre de virus DOS, néanmoins ils sont considérés comme une plus grande menace que les virus DOS puisque la plupart des ordinateurs fonctionnent maintenant sous Windows.

5.4.4 Virus Macintosh

La plupart des virus Macintosh connus à ce jour sont bénins et ne détruisent rien, ils se contentent d'afficher des images ou des messages.

[21] "Windows Malware Analysis Essentials"

Victor Marak, Sarath Geethakumar, et Samir Datt

Les virus Macintosh sont spécifiques au mac et ne peuvent infecter des programmes Windows. Le nombre de virus Macintosh est assez réduit due à la complexité du système d'exploitation MacOS.

5.4.5 Virus Macro

Les virus Macros sont la plus grande menace à ce jour, ils se propagent lorsqu'un document Microsoft Word, Excel ou PowerPoint contaminé est exécuté.

Un virus Macro est une série de commandes permettant d'effectuer un certain nombre de tâches automatiquement au sein des applications ci-dessus.

Le but non nuisible du langage de macro dans ces applications est à l'origine de pouvoir créer des raccourcis pour effectuer des tâches courantes, par exemple en une touche imprimer un document, le sauvegarder et fermer l'application.

5.4.6 Virus Polymorphe

Ceci est une sous-catégorie, dans le sens ou n'importe lequel des types de virus ci-dessus peut en plus être polymorphe.

Les virus polymorphes incluent un code spécial permettant de rendre chaque infection différente de la précédente.

Ce changement constant rend la détection de ce type de virus compliqué.

Souvent le code change, mais l'action pour lequel il a été créé est toujours la même.

Par exemple, le virus peut intervertir l'ordre des instructions de son action en son sein, ou rajouter de fausses instructions afin de tromper la vigilance de l'antivirus, qui lui, recherche une signature précise.

Beaucoup de virus polymorphes sont aussi encryptés. Le virus encryptera son code et ne le décryptera que lorsqu'il doit infecter un nouveau fichier, le rendant encore plus difficile à détecter.

5.4.7 Virus Furtif

Un virus furtif, comme son nom l'indique, va se cacher lorsque l'ordinateur ou l'utilisateur accède au fichier infecté.

Si l'utilisateur ou l'antivirus tente de voir si le fichier est infecté, le virus le saura et va se cacher offrant à l'antivirus et à l'utilisateur une version non infectée du fichier.

5.4.8 Virus Multi cibles

Les virus multi cibles utilisent à la fois les techniques d'infection des virus programmes et ceux de zone d'amorce. Ils infecteront donc à la fois les zones d'amorces et les programmes.

Ces virus ont tendance à avoir une taille un peu plus élevée que les autres types puisqu'ils doivent contenir les instructions pour effectuer deux types d'infections.

En doublant l'infection, le virus double sa chance d'être transmis à un autre ordinateur et de se répandre.

Ceci explique qu'ils sont responsables d'un grand nombre d'infections, sans être très nombreux.

5.4.9 Virus résidents [22]

Les virus résidents sont des virus qui se chargent en RAM et qui infectent les fichiers au fil du temps lors de leur ouverture ou exécution. Les plus récents de ces virus prennent souvent la forme d'un pilote virtuel sous Windows (.vxd). Ils sont alors chargés par le système d'exploitation lui-même et avant les anti-virus. Ceci les rend plus difficiles à détruire.

5.4.10 Virus de fichiers exécutables

Ces virus disposent d'une fonction d'altération des fichiers exécutables présents sur les disques de la machine infectée. Ces virus utilisent plusieurs techniques d'infection :

- Virus par recouvrement : Ces virus écrasent le début des programmes cibles avec leur propre code machine. Le programme cible est alors inutilisable.

Le seul avantage de cette technique est que la taille du code n'est pas modifiée.

- Virus par ajout : Ces virus altèrent le début du programme infecté pour faire exécuter le code viral en premier. Ce code est ajouté à la fin du fichier. La taille du fichier est modifiée.
- Virus par entrelacement : Cette technique est plus fine que les deux précédentes. Il s'agit alors d'insérer le code malicieux dans des zones non utilisées du programme.

Ces zones sont typiquement entre les blocs du programme (code, données et pile).

5.4.11 Virus compagnons

[22] "Computer Viruses and Malware"

John Aycock

Les virus compagnons sont des virus portant le même nom qu'un autre programme et qui utilisent la précédence des extensions. En effet, si l'on veut utiliser un programme, qu'il existe dans le chemin un programme et que l'on appelle prg sans extension, c'est qui s'exécutera.

Le virus compagnon utilise donc un nom de fichier du système ou courant en substituant l'extension .com à .exe. Il s'exécutera donc à la place de l'exécutable réel en .exe lors d'un appel sans précision de l'extension.

Le virus compagnon peut, ou non, être dans le même répertoire que sa cible. Il suffit qu'il soit dans un répertoire situé dans la variable PATH. Ces virus sont apparentés aux chevaux de Troie.

5.4.12 Virus défensifs

Ces virus sont capables de désactiver ou détruire certains anti-virus. Ils sont donc capables de se propager sans être détectés.

5.4.13 Virus mailers et mass-mailers

Ces virus sont capables d'utiliser la messagerie électronique pour se propager. Les virus mailers envoient un mail à chaque activation. Les virus mass-mailers envoient plusieurs mails à chaque activation

6. Spam [23]

L'ouverture de nouveaux services par Internet est souvent l'occasion pour des pirates de tester leur sécurité. Dans le cas de la messagerie, la situation est particulièrement délicate en raison de la nature même la messagerie qui utilise des protocoles de transfert Internet (SMTP : Simple mail transfert protocole). En effet, il est pratiquement impossible d'empêcher l'envoi de contenus subversifs, l'envoi de message collectifs (et la constitution de groupes favorise cela), ou encore l'usurpation d'une identité….

6.1 Définition

On définit le Spam comme une attaque visant à crasher un programme en faisant déborder un tampon (buffer) de taille fixe avec un trop grand nombre de données entrantes.

[23] "The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders, and Deceivers" Kevin D. Mitnick et William L. Simon

Peut aussi servir à submerger (flood) une personne ou un newsgroup avec des messages sans rapport avec les autres ou inappropriés.

6.2 Buts

Le but premier du Spam est de faire de la publicité à moindre prix par « envoi massif de courrier électronique non sollicité « (junk mail) ou par « multi postage abusif » (EMP).

6.3 Effets du Spam

Le principal inconvénient du Spam est l'espace qu'il occupe dans les boites aux lettres des victimes et la bande passante qu'il gaspille sur le réseau Internet.

7. Mail-bombing

7.1 Définition

Le Mail-bombing consiste à envoyer un nombre faramineux d'emails (plusieurs milliers par exemple) à un ou des destinataires.

En effet les mails sont stockés sur le un serveur de messagerie, jusqu'à ce qu'ils soient relevés par le propriétaire du compte de messagerie.

Ainsi lorsque celui –ci relèvera le courrier, ce dernier mettra beaucoup trop de temps et la boite aux lettres deviendra alors inutilisable ….

7.2 Objectif

L'objectif étant de :

- Saturer le serveur de mails

Figure 23 : communication client-serveur par socket

- Saturer la bande passante du serveur et du oui des destinataires,
- Rendre impossible aux destinataires de continuer à utiliser l'adresse électronique.

Section 3 : LES AUTRES FORMES DE MENACE

1. Ingénierie Sociale (Social Engineering) [24]

Le terme d'ingénierie sociale » (social engineering) désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité.

Il exploite la « faiblesse humaine » et permet de récupérer plus facilement et plus rapidement des informations que par une attaque « logique » avec technique.

Contrairement aux autres attaques, elle ne nécessite pas de logiciel. La seule force de persuasion est la clé de voûte de cette attaque.

Il y a quatre grandes méthodes de social engineering : par téléphone, par lettre, par Internet et in « situ ».

1.1 Le social engineering par téléphone

Le cas le plus typique de social engineering est la récupération d'information par téléphone.

Par exemple, l'attaquant commence par se renseigner au préalable sur la société, en recherchant des informations pertinentes via Internet : numéros de téléphone, nom, prénom, fonction des responsables de la société ou encore des informations relatives aux administrateurs du système d'information.

L'attaquant va ensuite téléphoner et se substituer à une personne, un administrateur par exemple.

Il prendra soin de donner quelques informations faisant penser à la victime qu'il appartient à l'entreprise ou qu'il est bien la personne qu'il prétend être. Ensuite, il va utiliser différentes manoeuvres psychologiques pour soutirer des informations. Il peut, par exemple, commencer à perturber la victime en lui indiquant qu'un virus très dangereux sévit sur sa machine et demander à cette personne d'effectuer des opérations plus ou moins complexes.

[24] "The Art of Deception: Controlling the Human Element of Security"

Kevin D. Mitnick

Une fois que la victime est en disposition psychologique plus faible (stress), l'attaquant peut alors lui proposer qu'elle lui donne le login et le mot de passe pour qu'il fasse les manipulations à sa place.

La victime, soulagée, sera alors bien contente de donner son mot de passe, sans forcément s'apercevoir du piège.

Les services clients (« help-desk ») sont particulièrement vulnérables, car les employés sont entraînés à être serviables et à dépanner les utilisateurs. Il peut être facile de dire qu'on a oublié son mot de passe et qu'on a un travail très urgent à terminer.

La personne du service client sera alors tentée d'effectuer une opération permettant l'accès illégitime. Le « social engineering » par téléphone peut également passer par le piratage du PABX de l'entreprise. L'attaquant pourra ainsi faire croire qu'il appelle de l'intérieur de l'entreprise, ce qui lui apporte un gain de confiance par rapport à sa victime.

1.2 Le social engineering par lettre

L'hacker vous fera une lettre très professionnelle. Au besoin, il n'hésitera pas à voir un imprimeur pour avoir du papier à lettre comportant un logo, un filigrane, téléphone, fax, email Il utilisera très certainement une boîte postale pour l'adresse de sa société fictive.

1.3 Le social engineering par internet

Le social engineering par Internet est semblable à celui par téléphone. Le hacker se fera facilement passer pour un opérateur système, un responsable informatique ou un ingénieur système.

1.4 Le social engineering « in situ »

Le « social engineering » peut également être pratiqué dans les locaux même de l'entreprise.

Le pirate ou l'espion industriel peut pratiquer du social engineering pour accéder aux locaux : un sourire avenant, une forte assurance, une décontraction certaine, costard, cravate, très classe, très propre, attaché-case, agenda rempli, documents divers, carte de visite, badge Ensuite, il n'a qu'à fureter à droite à gauche, rentrer dans les bureaux vides, aller voir du côté des imprimantes et jeter un oeil dans les poubelles pour trouver des informations intéressantes.

2. Le Reverse Social Engineering (RSE)

Le « reverse social engineering » est une manoeuvre beaucoup plus complexe qui consiste à inverser la situation.

Par exemple, ce n'est pas l'attaquant qui appelle pour récupérer des informations, mais la victime qui appelle l'attaquant pour les lui donner !

Un cas typique de « reverse social engineering » consiste pour l'attaquant à saboter une machine à laquelle il a accès par d'autres moyens. La victime qui s'aperçoit que la machine ne marche plus, va vouloir appeler quelqu'un pour l'aider.

L'attaquant aura pris soin de faire savoir qu'il était capable de réparer les dégâts (en en parlant autour de lui, en laissant traîner des cartes de visite, en mettant un message d'erreur demandant explicitement de l'appeler en cas de panne, etc.).

La victime appellera alors l'attaquant et sera toute disposée à lui confier des informations sensibles :

Numéro de contrat de support, login, mot de passe

3. Loteries

Vous recevez un courrier électronique indiquant que vous êtes l'heureux gagnant du premier prix d'une grande loterie d'une valeur de plusieurs (centaines de) milliers d'euro.

Pour empocher le pactole il suffit de répondre à ce courrier. Après une mise en confiance et quelques échanges de courriers, éventuellement avec des pièces jointes représentant des papiers attestant que vous êtes bien le vainqueur, votre interlocuteur vous expliquera que pour pouvoir toucher ladite somme, il faut s'affranchir de frais administratifs, puis viennent des frais de douane, des taxes diverses et variées, etc.

C'est de cette façon que ces cyber truands arrivent à extorquer des milliers d'euros à des internautes dupes de cette supercherie.

4. Scam [25]

Le «scam» («ruse» en anglais), est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage.

[25] "Scam Me If You Can: Simple Strategies to Outsmart Today's Rip-off Artists" Frank Abagnale

Cette arnaque est issue du Nigeria, ce qui lui vaut également l'appellation «419» en référence à l'article du code pénal nigérian réprimant ce type de pratique.

L'arnaque est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer les fonds.

Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds. En répondant à ce type de message l'internaute s'enferme dans un cercle vicieux pouvant lui coûter de quelques centaines d'euro s'il mord à l'hameçon et même la vie dans certains cas. En effet, deux cas de figures se présentent :

- Soit les échanges avec l'escroc se font virtuellement auquel cas celui-ci va envoyer quelques "documents officiels" pour rassurer sa victime et petit à petit lui demander d'avancer des frais pour des honoraires d'avocats, puis des frais de douanes, des frais de banque, etc.
- Soit la victime accepte, sous pression du cyberbandit, de se rendre dans le pays avec la somme en liquide auquel cas elle devra payer des frais pour pouvoir rester dans le pays, payer des frais de banque, soudoyer des hommes d'affaires, et ainsi de suite.

Dans le meilleur des cas la victime rentre chez elle en avion délestée d'une somme d'argent non négligeable, dans le pire scénario plus personne ne la revoit jamais.

5. Les intrusions systèmes

On peut regrouper les attaques par intrusion en 2 types :

- Les intrusions directes.
- Les attaques « man in the middle. »

5.1 Les intrusions directes

C'est la plus simple des attaques. L'hacker s'introduit directement vers sa victime à partir de son ordinateur

5.2 Les attaques « man in the middle. »

L'attaque "Man In The Middle" ou « Attaque de l'homme au milieu » s'agit d'un type d'attaque où une tierce personne s'interpose de manière transparente dans une connexion pour écouter ou s'introduire dans un système sans se faire remarquer.

Il existe plusieurs méthodes pour cela :

5.2.1 Le Hijacking [26]

Ce type d'attaque est fondé sur une faiblesse de TCP/IP, il consiste à désynchroniser une connexion entre deux machines à partir d'une troisième machine.

Une fois cette manoeuvre réussie, l'intrus a usurpé l'identité de la machine désynchronisée.

5.2.2 Le TCP-SYN flooding

Cette technique d'attaque exploite la particularité du mode d'établissement des connexions de TCP

. Lors de l'établissement d'une connexion, serveur et client échangent des informations, en même temps. Au cours de cette phase d'établissement des connexions restent semi-ouvertes sur le serveur dans l'attente d'accusé de réception du client. C'est la porte que recherche le pirate pour pénétrer sur le réseau

. Pour obtenir cette situation, il va susciter l'ouverture de session sur le serveur, en utilisant souvent le relais d'une machine faiblement protégée.

5.3 L'observation du réseau.

5.3.1 L'examen des paquets (sniffing)

Un réseau à support partagé est un réseau dans lequel les paquets sont transmis partout sur le réseau quand ils circulent de l'origine vers les points de destination.

La capture de ces paquets est appelée "observation de réseau" ou "reniflement de paquets" ou encore "interception illégale".

Si un renifleur *(sniffer)* ou encore analyseur de protocoles est installé n'importe où le long du chemin entre une machine origine et une machine destination, les informations de connexion peuvent être saisies et utilisées ensuite pour attaquer la machine de destination. L'observation du réseau est une des menaces les plus sérieuses pour les entreprises.

5.3.2 Le détournement de session

[26] "Hacking: The Art of Exploitation"

Les techniques de hijacking

Jon Erickson

Le détournement de session est une variante du spoofing IP. Un intrus cherche une communication réelle entre deux stations et essaie de prendre le pouvoir.

Après avoir pris le contrôle d'une station (un firewall ou un composant dans un réseau de prestataire de service) par laquelle passe la communication ou une autre machine sur le même réseau local que celui d'une des deux machines, l'intrus observe la communication comme il veut. Ainsi il peut déterminer les numéros de séquence utilisés.

Ensuite il génère le trafic qui semble venir de l'une ou l'autre des deux machines en volant effectivement la session de l'un des deux correspondants pour avoir les mêmes privilèges d'accès que l'utilisateur légitime.

Après avoir éliminé l'utilisateur légitime de la communication, il peut maintenant continuer ce que l'utilisateur original a commencé.

5.4. Les contres mesures

La création d'une stratégie de sécurité[27] du site consiste à établir une liste de tous les éléments à protéger. Cette liste doit pouvoir être mise à jour facilement et régulièrement. Les éléments à considérer comprennent :

- Matériel : unités centrales, cartes, claviers, terminaux, stations de travail, ordinateurs personnels, imprimantes, lecteur de disquette, lignes de transmission, serveurs de terminaux, routeurs.
- Logiciel : programmes applications, utilitaires, programmes de diagnostic, systèmes d'exploitation, programmes de communication.
- Données : pendant l'exécution, stockées en ligne, archivées hors ligne, sous forme de sauvegardes, listes de contrôle et bases de données, en transit sur supports de communication.
- Personnes : utilisateurs, personnel nécessaire à l'exploitation des systèmes. Documentation:

Sur les programmes, le matériel, les systèmes, les procédures administratives locales.

- Fournitures : papiers, formulaires, rubans, supports magnétiques.

Puis vient ensuite la protection proprement dite :

[27] "Information Security Management Principles"

La création d'une stratégie de sécurité

David Alexander, Mandy Andress, et Richard Boddington

5.4.1. Réduire l'accès au réseau par l'utilisation d'un firewall [28]

Les systèmes "Firewall" protègent et facilitent l'utilisation de réseau à plusieurs niveaux.

• Ils permettent la mise en place d'un courrier électronique et d'autres applications telles que le système ftp et la connexion à distance, même s'ils limitent l'accès au réseau interne.

• Ils constituent un dispositif d'autorisation, garantissant un niveau de sécurité, dans la mesure où seuls des utilisateurs ou des applications spécifiées peuvent se connecter via le système "Firewall".

• Ils possèdent généralement une fonction de journalisation et d'alarme, permettant le suivi d'une utilisation identifiée et de signaux lors d'événements précis.

• Ils permettent la traduction d'adresses, qui masquent l'adresse et le nom réels de toute machine transmettant des données par le dispositif "Firewall". Par exemple, pour tous les messages adressés à une personne appartenant au service d'assistance technique, les adresses se transformeront en , afin de cacher efficacement le nom d'un utilisateur réel et d'une adresse de réseau.

• Ils permettent d'ajouter de nouvelles fonctions, telles que le chiffrement et les capacités de réseau privé virtuel. Le chiffrement consiste à coder ou à verrouiller les données et à empêcher la lecture d'informations par des utilisateurs non autorisés. Les réseaux privés virtuels (VPN) utilisent le chiffrement pour permettre des transmissions fiables sur les réseaux publics (comme le réseau Internet).

• Les systèmes "Firewall" peuvent également être développés au sein du réseau d'une entreprise afin de compartimenter différents serveurs et différents réseaux, et ainsi de contrôler les accès au sein du réseau. Une entreprise peut souhaiter, par exemple, séparer le "serveur comptabilité et fiches de salaire" du reste du réseau, pour n'autoriser que certains individus à accéder à ces informations.

5.4.2 Installer et mettre à jour régulièrement un logiciel d'antivirus

[28] "Firewalls and Internet Security: Repelling the Wily Hacker"

La configuration et la gestion des pare-feu

William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin

2.1 Automatisation

Plusieurs antivirus existent sur le marché : les antivirus professionnels et les antivirus personnel. Mais le meilleur antivirus du monde n'a de sens que si l'organisation assure sa mise à jour régulière. En effet de nouveaux virus voient le jour quotidiennement. Alors il serait préférable d'utiliser des antivirus qui assurent leur mise à jour automatique.

5.4.2.2 Vérification

De manière périodique, l'administrateur réseau doit procéder à la vérification de la date de dernière mise à jour sur les postes de travail. En effet, il suffit parfois de peu de chose pour bloquer la fonction de mise à jour automatique et les utilisateurs ne s'en rendront souvent pas compte.

6. Surveiller les flux d'informations

Les flux d'informations dans votre système réseau doivent êtres connus et surveiller pour des raisons de sécurité, de disponibilité et de coût. Un trafic anormal peut révéler une intrusion ou un système défectueux. Généralement ce sont des logiciels spécialisés installés sur les serveurs qui peuvent visualiser ces flux que ce soit local ou en réseaux.

7. Contrôler les documents provenant de l'extérieur

Toute pièce jointe doit faire l'objet d'une analyse par un antivirus récent avant d'être ouverte par un utilisateur. L'antivirus peut être centralisé (sur le serveur) ou local (sur les postes de travail).

8 Définir une politique de sécurité interne

8.1 Nécessité d'authentification et d'identification

Ces procédés permettent de savoir si un interlocuteur est bien celui qu'il prétend être. Les demandes de nom et de mot de passe utilisés pour filtrer l'accès à un site ou un document sont une forme d'authentification mais d'autres sont encore plus poussées, comme l'identification du PC ou de la carte réseau, du numéro de ligne téléphonique, …

Tous les utilisateurs d'un réseau devraient ainsi avoir un identifiant et un mot de passe unique et secret leur permettant, en entrant une seule fois leur code, un accès à toutes les informations auxquelles ils ont le droit.

L'authentification sert alors à :

- La protection contre les accès illicites,
- S'assurer de l'identité du demandeur,
- Garantir le bon destinataire,

8.1.1 Mots de passe

Les mots de passe permettent d'authentifier les utilisateurs lorsqu'ils se connectent au système informatique. Généralement, ils permettent de vérifier l'identité de l'utilisateur. Malheureusement, il existe certains moyens pour neutraliser un système de mots de passe :

- Un individu, désireux de se connecter, peut "écouter" un nom d'utilisateur et un mot de passe pendant qu'un utilisateur autorisé se connecte sur un réseau public.
- Un individu désireux de se connecter, peut s'attaquer à votre système d'accès en tapant un dictionnaire entier de mots (ou de plaques d'immatriculation ou toutes autres listes) dans un champ de mot de passe.
- Des utilisateurs risquent de communiquer leur mot de passe à un collaborateur ou risquent de laisser dans un endroit public une liste de mots de passe système.

Heureusement, il existe une technologie de mots de passe et d'outils permettant de rendre votre réseau plus fiable :

- La génération des mots de passe valables "une fois" est efficace dans des situations spécifiques de connexion à distance, car elles supposent qu'un mot de passe peut être neutralisé. Avant de quitter le réseau interne, le système génère une liste de mots de passe qui fonctionneront seulement une fois pour un nom d'utilisateur donné. Pour se connecter au système à distance, l'utilisateur ne peut utiliser son mot de passe qu'une seule fois, celuici cessant alors d'être valide.
- Les fonctions de système d'exploitation, telles que l'expiration des mots de passe et l'application d'une stratégie de mots de passe. L'expiration du mot de passe est une fonction obligeant l'utilisateur à créer régulièrement de nouveaux mots de passe. Une bonne stratégie de mots de passe consiste à définir un nombre minimal de caractères et un mélange des lettres et numéros. Le système d'exploitation ne pourra accepter un mot de passe s'il ne respecte pas ces règles.
- Les cartes à puce garantissent une protection particulièrement fiable des mots de passe. Le principe consiste à créer des mots de passe uniques sur un petit dispositif de type carte de

crédit, ledit système étant basé sur un principe "d'interrogations - réponses". Le mot de passe est ensuite tapé (procédure de connexion) et validé sur un serveur de mots de passe, qui gère tous les accès au système. Logiquement, ces systèmes sont souvent onéreux dans leur application.

8.1.2 Biométrie

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques (empreinte digital, empreinte rétinien…) .Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. La technique de biométrie est utilisée de préférence pour les opérations d'identification plutôt que d'authentification.

9. Crypter les données [29]

Que ce soit en liaison directe par modem, via un VPN, ou dans un échange e-mail, les communications entre le réseau et un PC distant peuvent être cryptées, c'est à dire chiffrées.

Ainsi l'émetteur est clairement identifié et son message est garanti intègre (non modifié depuis l'émission), de même que le récepteur. Cette méthode s'améliore chaque jour, avec des clés de cryptage de plus en plus longue, donc plus difficiles à percer.

10. Sécuriser les données

10.1 Accès physique

10.1.1 Serveur

Au-delà de la configuration des accès aux serveurs, l'accès physique à la machine est également crucial. Idéalement les serveurs se trouveront dans une pièce ignifugée et refroidie, fermée à clé et munie d'une alarme.

10.1.2 Réseau

[29] "Cryptography and Network Security: Principles and Practice"

Les bases de la cryptographie

William Stallings

Si les câbles du réseau sont apparents, il est assez simple d'en détourner un ou de récupérer les informations qui y circulent avec de petits appareils électroniques bon marché. C'est encore plus vrai dans les réseaux sans fils. On veillera donc à protéger les câbles dans des goulottes ou dans les murs et à disposer les panneaux techniques dans des endroits non accessibles au public.

10.1.3 Poste de travail

Lorsqu'un utilisateur est amené à sortir de son bureau, il est utile qu'il se déconnecte du réseau. En effet, n'importe qui peut s'asseoir derrière le PC toujours connecté et avoir accès aux mêmes informations que l'utilisateur. De même tous les postes de travail seront recensés, numéroté et peut être attachés physiquement aux murs ou aux bureaux dans le cas des PC portables, en particulier dans les lieux faciles d'accès (intrusion nocturne par exemple).

10.2. VPN [30]

Dès lors que l'accès est autorisé depuis l'extérieur (Internet…) il est intéressant de mettre en oeuvre un système de VPN (Virtual Private Networking). Ce système permet d'isoler une communication entre un poste client et un serveur, via Internet, pour rendre la communication la plus sécurisée possible. Un réseau privé virtuel est une sorte de tunnel privé qui traverse le réseau public, comme Internet, et qui permet de connecter les télétravailleurs à votre réseau ou vos sites distants entre eux. Les utilisateurs du réseau peuvent se connecter en toute confidentialité et partager les applications et les informations. Couplés aux firewalls ils permettent de restreindre l'accès à certaines ressources du réseau.

11. Sauvegarder les données

Les données sont installées en principe (qu'elles soient réparties ou non) sur des mémoires de masses (disques durs, bandes magnétiques, CD-RW, DVD-W). Des sauvegardes méthodiques (dépendant du service exploitation), l'utilisation de dispositifs spéciaux tels que disques miroirs permettent dans une large mesure d'éviter la perte (toujours préjudiciable) de données. Une des méthodes les plus efficaces consiste à sauvegarder sur bandes magnétiques selon une procédure définie :

Par exemple :

[30] "Virtual Private Networks (VPNs) : What Is a VPN, Why Would I Need One and How Do I Get Started?" Comprendre les VPN (Mike Meyers)

- Sauvegarde journalière (fichiers modifiés uniquement)
- Sauvegarde hebdomadaire (tous les fichiers utilisateur)
- Sauvegarde système journalière (fichiers système modifiés uniquement)
- Sauvegarde système hebdomadaire (tous les fichiers système)
- Sauvegarde mensuelle (tous les fichiers système et utilisateur)

Cette procédure est valable quel que soit le système utilisé (Mainframe, Mini, Micro-ordinateur).

12. Analyser les journaux d'activité

Afin de détecter les intrusions – internes et externes – dans votre système d'information, il est bon de connaître quel est le comportement « normal » de votre système. Ainsi, vous pourrez mettre en évidence tout changement suspect. La communication avec le monde extérieur se fait de plus en plus par Email.

Il est possible de garder un journal d'entrée et sortie de tous les e-mails transitant par votre serveur. Si les informations sont dites « sensibles », il est aussi possible d'archiver en temps réel tout le flux de courrier.

Les accès à vos serveurs de fichiers peuvent aussi être enregistrés dans les journaux de votre système, les « event logs ».

Enfin, il est parfois souhaitable de tracer l'utilisation d'un logiciel ou d'un fichier particulier.

En plus des rapports fournis par votre système d'exploitation, certains logiciels gardent une liste des accès enregistrant le nom de l'utilisateur et l'heure d'accès.

13. Tester les intrusions

Votre système une fois sécurisé doit être testé. Pour ce, vous devez « jouer » au hacker afin de vérifier que touts les accès sont bien contrôlé. Ce travail demande beaucoup d'imagination car le point faible de votre système est précisément celui auquel vous n'avez pas pensé. Ces tests doivent se réaliser de l'extérieur et de l'intérieur de votre système. Ces tests doivent être menés régulièrement.

14 . Conclusion

Nos systèmes sont interconnectés aux réseaux depuis longtemps. Lors du choix de l'architecture des points d'accès de ces systèmes aux réseaux, la sécurité n'était pas un critère prioritaire. Le but principal était alors la connectivité totale (full connectivité). On pensait qu'il pourrait y avoir des problèmes de sécurité dans le futur mais ce n'était pas prioritaire dans les choix techniques. Les réseaux n'étaient qu'un ensemble de moyen de recherche où « tout le monde se connaissait ». On n'avait pas d'attaque de spam, Trojan, virus, flood, spoofing, sniffer.

Maintenant les réseaux sont devenus des outils de communication mondiale, utilisés par des bons et mauvais citoyens et toutes les déviances courantes y sont présentes. On a pu voir rapidement que cette connectivité totale était une aubaine pour les personnes mal intentionnées qui pouvaient ainsi essayer très facilement de tester toutes les machines d'un site et découvrir rapidement un maillon faible afin de s'introduire facilement dans le système.

Lorsqu'une intrusion est constatée, les dégâts sont souvent importants et nécessitent un travail long et fastidieux pour remonter le système et supprimer les failles de sécurité. Tout cela affecte lourdement la continuité du réseau et du système d'information. Les méthodes et les outils qu'utilisent les pirates sont bien rodés et d'un accès malheureusement très facile ; des kits entiers de piratage circulent sur le réseau.

C'est pour cela que la sécurité des informations et des réseaux est alors devenu un concept primordial pour tout administrateur car je répète toujours et jamais assez:nul n'est à l'abri des menaces.

Chapitre 3 :

La sécurité des systèmes d'informations de la CASNOS

Introduction du chapitre 3

Dans le cadre de l'amélioration du service public, la Caisse nationale de sécurité sociale des non-salariés CASNOS a choisi la solution des guichets itinérants pour sillonner les localités éloignées ou dépourvues d'annexes CASNOS, afin d'attirer de nouvelles adhésions et élargir sa couverture aux non-salariés (commerçants, artisans, agriculteurs, éleveurs, transporteurs, médecins généralistes et spécialistes, avocats et autres professions libérales) sur la réception des dossiers médicaux d'assurés sociaux et fichiers des pharmaciens, les cartes CHIFA (réception des dossiers, remise et mise à jour des cartes), le système de retraite (réception des demandes de retraite), le renouvellement des dossiers de retraite et d'invalidité, le système de recouvrement, le contrôle médical, l'immatriculation, l'encaissement par le canal de la banque, le recours et la remise des mises à jour.

Pour cela, nous allons structurer ce chapitre en trois sections principales :

Section 1 : présentation de la casinos

Section 2 : Déterminer les systèmes d'information utilisés

Section 3 : Façons de protéger ces systèmes contre les menaces

Section 1 : présentation de l'entreprise casnos

1. Description de l'organisme d'accueil[31]

La mission et l'expansion de l'ex caisse d'assurance vieillesse des non-salariés (CAVNOS) furent interrompues par la promulgation du décret 223/85 du 20 Août 1985 portant sur l'unification des régimes de sécurité sociale qui intégra la CAVNOS dans le système global de solidarité sociale et dont les activités furent confiées selon les fonctions aux deux nouvelles caisses, la caisse nationale des assurances sociales et des accidents du travail (C.N.A.S.A.T) et la caisse nationale des retraites (C.N.R).

Après sept (07) ans de gestion unique et face aux réalités socio-économique et aux spécificités du secteur des non-salariés, le système de la Sécurité Sociale fut restructuré.
Cette nouvelle organisation visait à renforcer et à stimuler ce secteur et a mettre en évidence une volonté de maîtrise et de rigueur caractérisée par :

- Une structure hiérarchique plus décentralisée
- Un sentiment plus affirmé de ses responsabilités collectives
- Un grand souci de développement de ses ressources humaines
- Une volonté plus vigoureuse de décentralisation fonctionnelle
- Une simplification des relations avec l'assuré

2. Historique de la CASNOS

La sécurité sociale a été introduite en Algérie par la décision N°49/045 du 11 avril 1949 rendue exécutoire par l'arrêté du 10 juin 1949.

Depuis sa création à nos jours le de securité sociale a connu un développement intense et continu, plus précisément depuis l'indépendance du pays en 1962. De grandes améliorations ont été enregistrées, parmi lesquelles nous citerons notament la tendance à la génération de la protection sociale par son extension à de larges catégories, la simplification des formalités pour l'ouverture des droits.

Le régime des non-salariés existe en Algérie depuis 1958. Il n'a été au départ et jusqu'en 1974 qu'un régime particulier deretraite.
Depuis sa création ce régime a connu trois (03) phases importantes :

[31] https://damancom.casnos.dz/

2.1.1ère Phase / du 01 janvier 1958 au 31 décembre 1970[32]

L'arrêté du 30/12/1957 avait pour objet de préciser les modalités d'application du décret du 24/11/1956 portant institution en Algérie du régime d'allocation vieillesse pour chacune des organisations professionnelles désignées ci-après, ne bénéficiant pas du régime des salariés ou assimilés

- Professions Industrielles et Commerciales
- Professions Libérales
- Professions Artisanales
- Professions Agricoles

Par arrêté ministériel du travail et des affaires sociales du 08 Mars 1963 les trois (03) caisses régionales ont été fusionnées en une seule caisse C.A.V.C.I.A. " Caisse d'Assurance Vieillesse des Commerçants et Industriels d'Algérie " avec pour siège social Alger.

2.2.2ème Phase / du 01 janvier 1971 au 31 décembre 1973

Promulgation du décret N°70/116 du 1er Août 1970 portant organisation administrative des organismes de sécurité sociale.
L'organisation du régime non-agricole, du régime des fonctionnaires, du régime minier et du régime des non-salariés des professions non agricoles de sécurité sociale, comprend les organismes ci-après

- Une Caisse Nationale de Sécurité Sociale
- Des Caisses Régionales de Sécurité Sociale
- Une Caisse d'Assurance Vieillesse des Non-Salariés (C.A.V.N.O.S.)
- Une Caisse de Sécurité sociale des Fonctionnaires (C.S.S.F.)
- Une Caisse de Sécurité Sociale des Mineurs (C.S.S.M.)

2.3. 3ème Phase / Loi du 02 Juillet 1983

[32] https://damancom.casnos.dz/

Sous l'emprise de la législation en vigueur au 31 Décembre 1983, il existait huit (08) régimes de sécurité sociale, à savoir :

Le régime général non – agricole géré par la caisse Algérienne d'assurance vieillesse « C.A.A.V. »

- Le régime des mines géré par la caisse de sécurité sociale des mineurs « C.S.S.M. »
- Le régime agricole géré par la caisse nationale de mutualité agricole « C.N.M.A. »
- Le régime des cheminots géré la caisse des cheminots « C.C. »
- Le régime des marins pêcheurs (Gens de Mer) géré par l'établissement nationale des marins pêcheurs (E.N.M.G.)
- Le régime de la SONELGAZ géré par la caisse d'assurance et de prévoyance des agents de la SONELGAZ « C.A.P.A.S. »
- Le régime des fonctionnaires géré par la caisse sécurité sociale des fonctionnaires pour le volet assurances sociales et la caisse générale des retraités Algériens « C.G.R.A. » pour la partie retraite des fonctionnaires de la fonction publique
- Le régime des non-salariés géré par la caisse d'assurances vieillesse des non-salariés « C.A.V.N.O.S »

Ces lois ont été promulguées le 02 Juillet 1983 et applicables à compter du 1er Janvier 1984. Cependant, et en l'absence des textes d'application et devant le vide juridique, deux circulaires d'application sont intervenues, la première en Mai 1984 modifiée et complétée par la seconde circulaire de Mai 1985. Ces deux circulaires ont été modifiées et complétées par la circulaire générale d'application des lois de sécurité sociale du 10 Novembre 1991.

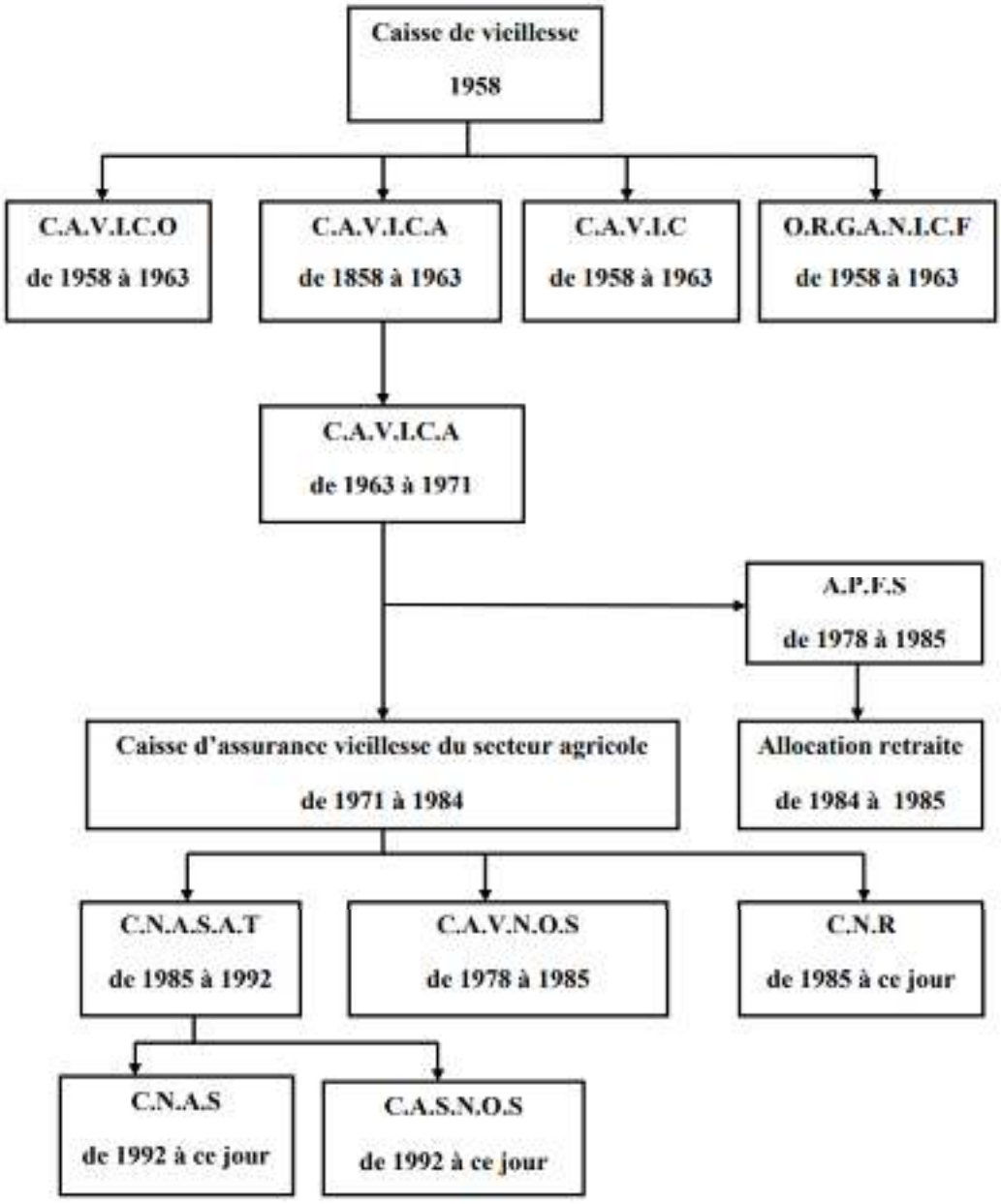

Figure 24 : Historique de la CASNOS (Etat récapitulatif).

3. Les missions de la CASNOS [33]

Dans le cadre des lois et règlements en vigueur, la caisse a pour mission :

- De gérer les prestations en nature et en espèces des assurances sociales des non-salariés.
- De gérer les pensions et allocations de retraites des non-salariés.
- De gérer jusqu'à extinction des droits des bénéficiaires les pensions et allocations servies au titre de la législation antérieure au 1er janvier 1984
- D'assurer le recouvrement, le contrôle et le contentieux du recouvrement des cotisations destinées au financement des prestations prévues aux alinéas précédents.
- De gérer, le cas échéant, les prestations dues aux personnes bénéficiaires des conventions et accords internationaux de sécurité sociale.
- D'organiser, de coordonner et d'exercer le contrôle médical.
- D'entreprendre des actions sous forme de réalisations à caractère sanitaire et social telles que prévues à l'article 92 de la loi n° 83-11 du 2 juillet 1983 susvisée, après proposition du conseil d'administration de la caisse.
- D'entreprendre des actions de prévention, d'éducation et d'information sanitaire après proposition du conseil d'administration,
- De gérer le fonds d'aide et de secours prévu à l'article 90 de la loi n° 83-11 du 2 juillet 1983 susvisé.
- De conclure, en coordination avec les caisses de sécurité sociale concernées, les conventions prévues à l'article 60 de la loi n° 83- 11 du 2 juillet 1983 susvisé.
- De procéder à l'immatriculation des assurés sociaux bénéficiaires.
- D'assurer en ce qui la concerne, l'information des bénéficiaires.
- De rembourser les dépenses occasionnées par le fonctionnement des diverses commissions ou juridictions appelées à trancher suite à des litiges nés des décisions rendues par la caisse.
- Des services du contrôle et du contentieux du recouvrement.
- De conclure des ententes avec les caisses de sécurité sociale en vue d'assurer le contrôle médical et le service des prestations.

[33] https://damancom.casnos.dz/

4. Organisations du CASNOS [34]

La C.A.S.N.O.S est organisée sur le modèle d'une structure centrale relayée par des agences de wilaya regroupant une à plusieurs antennes qui sont elles-mêmes relayées par des guichets de proximité (Arrêté Ministériel N°17 du 15/01/2015 portant organisation interne de la C.A.S.N.O.S.).

Sous l'autorité du Directeur Général, assisté du Directeur Général Adjoint et de Conseillers, la Direction Générale de la Caisse comprend

- La Direction des opérations financières
- La Direction des Prestations
- La Direction du Recouvrement, du Contrôle et du Contentieux
- La Direction des Ressources Humaines et des Moyens
- La Direction de la Modernisation et des Systèmes d'Information
- La Direction du Contrôle Médical, des Études et du Conventionnement
- La Direction de l'Audit et du Contrôle
- La Cellule des Études Actuarielles
- La Cellule d'Information et de Communication
- La Cellule d'Accueil, d'Écoute et de l'Orientation du citoyen
- La Cellule des Affaires Juridiques
- La Cellule des Archives et de la Documentation

Concernant la présence de la CASNOS à travers le territoire national, elle est structurée comme suit :

49 agences de wilaya auxquelles sont rattachées les antennes et les guichets de proximité.

[34] https://damancom.casnos.dz/

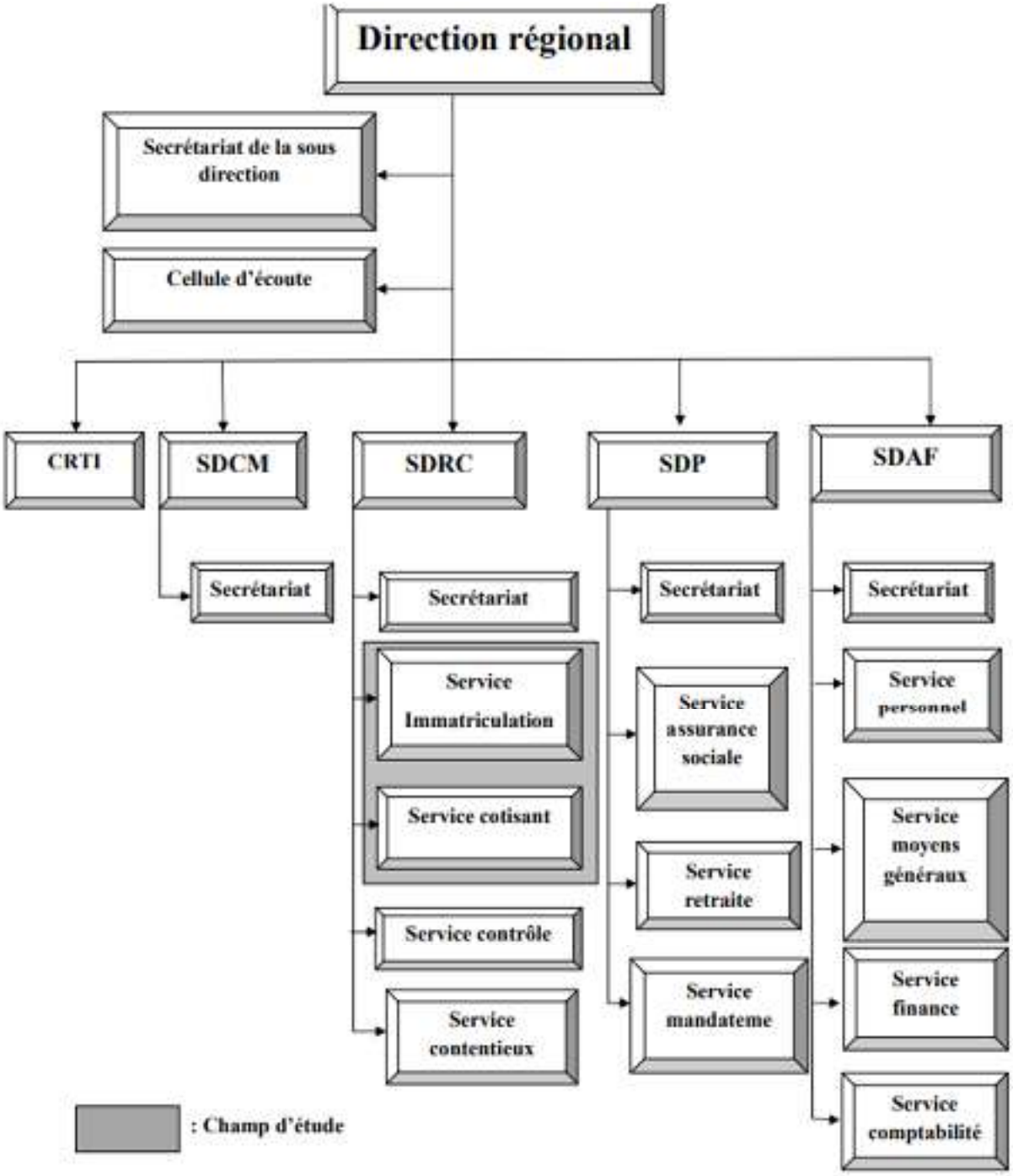

Figure 25 : Organigramme simplifié de la CASNOS

5. Mode d'organisation : [35]

- ✓ **Direction régionale :**

Il est nommé par le siège, assure la coordination de toutes les tâches des antennes.

- ✓ **Secrétariat de la direction régionale :**

Est la collaboratrice du directeur. Elle organise le travail administratif et favorise la communication à l'intérieur et à l'extérieur de l'entreprise. Elle effectue des travails classiques: frappe, saisit, rédige…, réceptionne les courriers et programme les rendez-vous.

- ✓ **Cellule d'écoute :**

Cette cellule est un outil mis à la disposition de l'ensemble des non-salariés. Elle constitue un intermédiaire entre l'assuré et l'administration qui a pour but d'améliorer la communication entre la caisse et l'assuré et de faciliter l'accès des non-salariés actifs et retraités.

- ✓ **Sous-direction de contrôle médical (SDCM):**

Elle est composée d'un médecin chef et de deux médecins conseils qui ont pour mission de confirmer les droits aux nouveaux malades chroniques et contrôlent les abouts.

- ✓ **Centre régionale de traitement informatique(CRTI) :**

Ce service comporte trois ingénieurs qui sont chargés de veillés à ce que l'informatique soit au service de tout le département en assurant la bonne connexion réseau et une haute disponibilité du système d'information.

- ✓ **Sous-direction de recouvrement et du contentieux (SDRC):**

Elle est chargée de suivre et d'organiser la gestion d'immatriculation pour les nouveaux cotisants, de suivre leur recouvrement du conformément aux lois règlements en vigueur, contrôle et vérifier leur déclaration de versement et les poursuivre dont le cas de l'absence de long terme et de négligence dans le paiement.

Pour cela, cette sous-direction dispose d'une secrétaire de direction et de quatre service :

• Service immatriculation.

[35] Service Personnel .

• Service cotisant.

• Service contrôle.

• Service contentieux.

✓ **Sous-direction des prestations(SDP) :**

Elle est chargée d'organiser et de suivre la gestion des prestations « assurance sociale » et des pensions de retraite des non-salariés, de gérer les droits du bénéficiaire.

Pour cela cette sous-direction dispose d'une secrétaire de direction et de trois service :

• Service d'assurance sociale.

• Service retraite.

• Service mandatement.

✓ **Sous-direction d'administration et finance (SDAF) :**

Elle comporte :

• Service personnel.

• Service des moyens généraux.

• Service finance.

• Service comptabilité.

5.1. Les responsables

- **Directeur :**

Est un responsable moral de l'unité qu'il dirige, il assure à la fois plusieurs missions ainsi l'apport de solutions aux problèmes techniques rencontrés par l'agence. Il est le véritable pilier de l'agence.

- **Sous-directeur de contrôle médical :**

Est le médecin chef national chargeait de l'orientation de la coordination et conseiller en matière de contrôle médicale.

- **Sous-directeur du recouvrement et du contentieux :**

Il assure la coordination et le suivi des opérations de toutes ses structures à travers l'échelle régionale (confection des statiques des encaissements et l'application de toutes les notes des services en matière du recouvrement et contentieux).

- **Sous-directeur des prestations :**

Il gère l'enveloppe des prestations des assurer et coordonne les travaux avec les guichets spécialisés.

- **Sous-directeur d'administration et finance :**

Il assure la gestion des recettes et dépenses, applique le budget de la caisse, coordonne les travaux de ses services et il analyse la situation des comptes bilans comptables.

- **Sous-directeur du centre régional de traitement informatique :**

Il est responsable de tout ce qui est gestion, construction, administration, surveillance et ingénierie des réseaux, et aussi il planifie, supervise et contrôle toutes les activités informatiques de l'agence.

5.2. Présentation de service immatriculation et service cotisant

Ces services font partie des services de la sous-direction de recouvrement et de contentieux. Le service immatriculation est chargé d'organiser la gestion d'immatriculation pour les nouveaux cotisants et recevoir des nouveaux dossiers, il est constitué de trois guichets, deux sont responsable de la création de nouveaux dossiers et le troisième s'occupe de la vérification. Le service cotisant s'occupe de contrôle des versements, il est constitué de six guichets, quatre sont responsable de payement des cotisations et deux pour la vérification.

6. Système d'information et l'entreprise

Un système d'information est l'ensemble des ressources (matériels, logiciels, données, procédures, ...) structurés pour acquérir, traiter, mémoriser, transmettre et rendre disponible l'information (sous forme de données, textes, sons, images, …) dans et entre les organisations.

Un système d'information est le véhicule de la communication dans l'entreprise (ou l'organisation), cette communication possède un langage dans les mots sont les données.

7. Fonctions des systèmes d'information dans l'entreprise :

- **Recueil de l'information :** Pour fonctionner, le système doit être alimenté par des informations qui proviennent de différentes sources internes ou externes.

- **Les sources externes :** C'est l'environnement du système, il s'agit généralement des flux en prévenance de partenaire (client, fournisseur, administration,) de plus, l'organisation doit être à l'écoute de son environnement pour anticiper les changements et adapter son fonctionnement.

7.1. Mémorisation de l'information :

Les informations stockées dans les ordinateurs sont sous forme de fichiers organisés afin d'être plus facilement exploitables sous la forme d'une base de données. Le système de gestion de la base de données(SGBD) est donc une composante fondamentale d'un système d'information.

7.2. Traitement de l'information :

Pour être exploitable, l'information subit des traitements, là encore les traitements peuvent être manuels ou automatiques. Les principaux types de traitement consistent à rechercher et à extraire, modifier, supprimer des informations.

7.3. Diffusion de l'information :

Pour être exploitée, l'information doit parvenir dans les meilleurs délais à son destinataire. Les moyens de diffusion sont : support papier (courrier, note interne), forme orale et support numérique qui garantit la vitesse de transmission optimale et la possibilité de toucher un maximum d'interlocuteurs. Ceci est d'autant plus vrai à l'heure d'internet et de l'interconnexion des systèmes d'information.

8. Les systémes d'informations utilisées par CASNOS

8.1. Le syscas [36]

[36] Service de recouvrement CASNOS

Figure 26 : Plateforme Syscas

C'est le système d'information qui prend en charge les tâches de recouvrement et contentieux. Recouvrement (Facturation) , elle est basé sur les documents fiscaux (bilan ; forfait) selon le statut c'est à dire une personne physique ou personne morale .

Dans le cas de personne morale : il y a le statut de l'entreprise et ainsi la notion des parts. On parle sur le recouvrement dès le 1 juillet de chaque année une majoration de retard c'est à dire une pénalité elle vaut 11% et chaque mois elle augmente de 1%. Il y a une autre pénalité elle s'appelle pénalité de retard de fausse déclaration chaque personne exerçant une activité non salariale doit déclarer cette activité dans un délai de 10 jours, une fois le délai est dépasser une pénalité de 5000 DA, en suite 1000 DA de chaque mois.

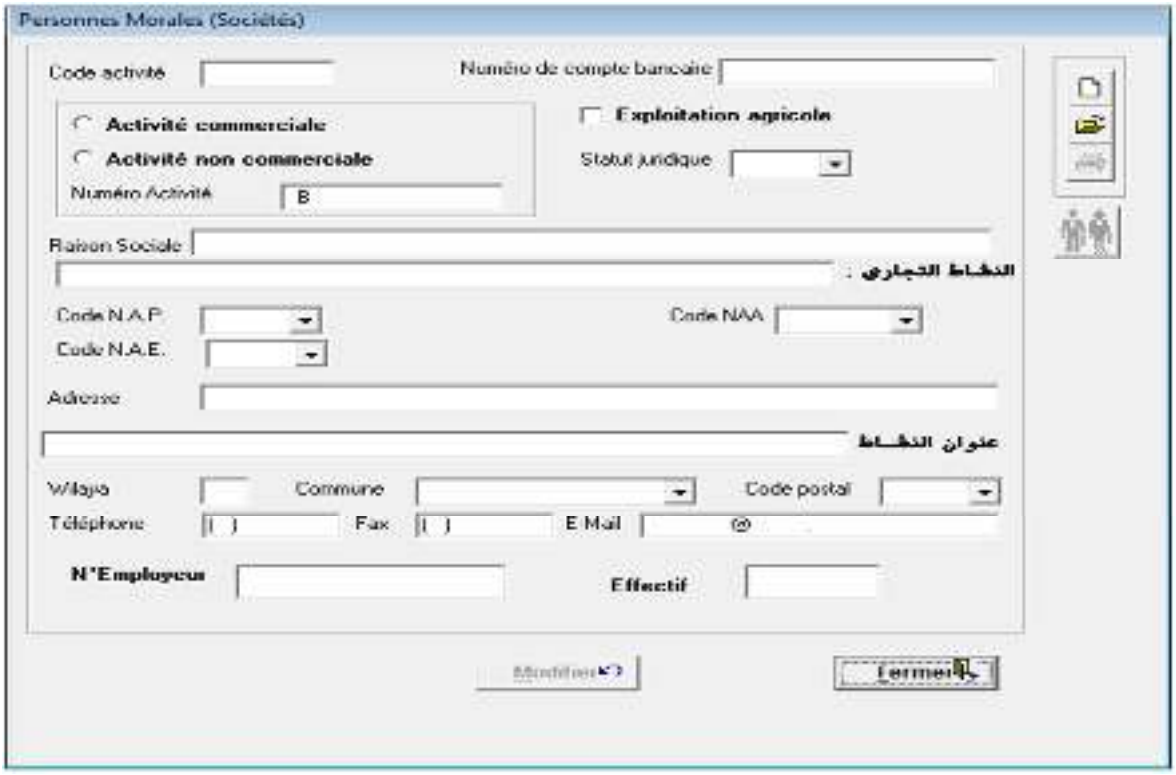

Figure 27 : Affiliation personne morale

Source : Service de recouvrement

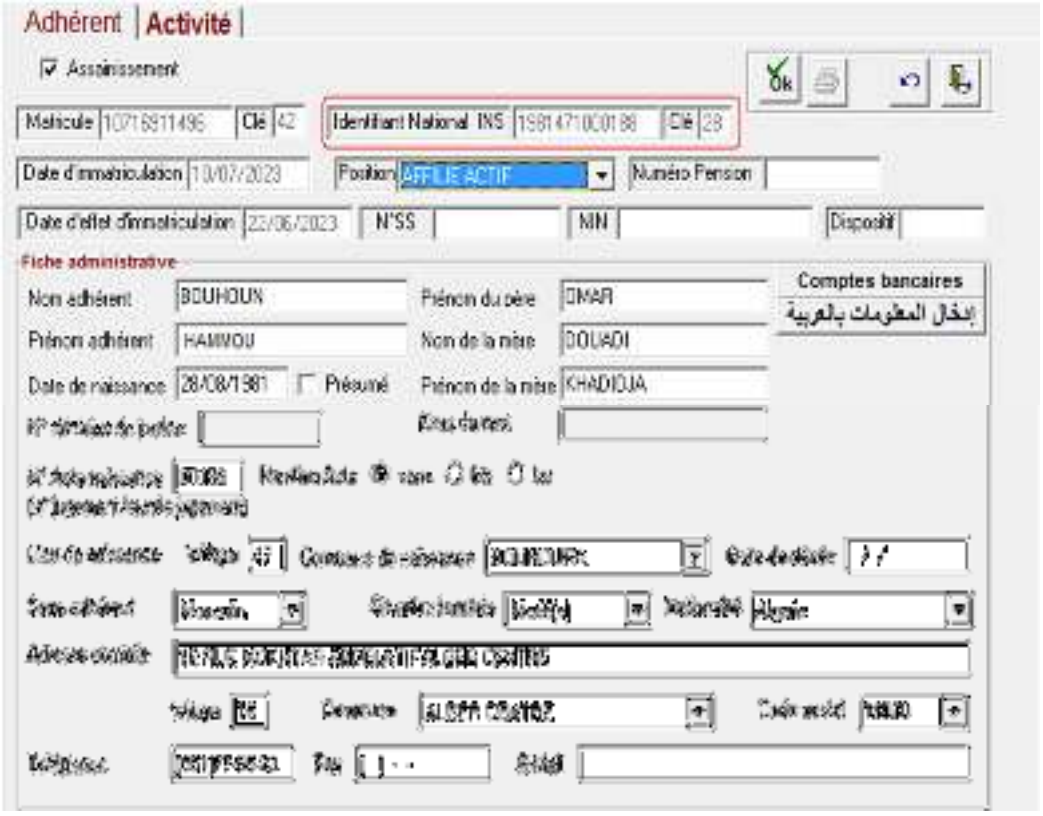

Figure 28 : Recherche adhérent

Source : Service de recouvrement

les mises en meures établis sont notifiés par huissier de justice ou par contrôleur agréé après un délai d'un mois si le concerné n'a pas payé ses cotisations une dossier de contentieux ouverte et systématiquement un processus bien déterminé sera engagé par le service contentieux tel que un avis avant pour suite juridique être envoyé au adhérent concerné sous 8 huitaine des procédures contentieuse seront exécutés à l'encontre de l'adhérent tel que l'opposition sur compte (poste ou bancaire) .

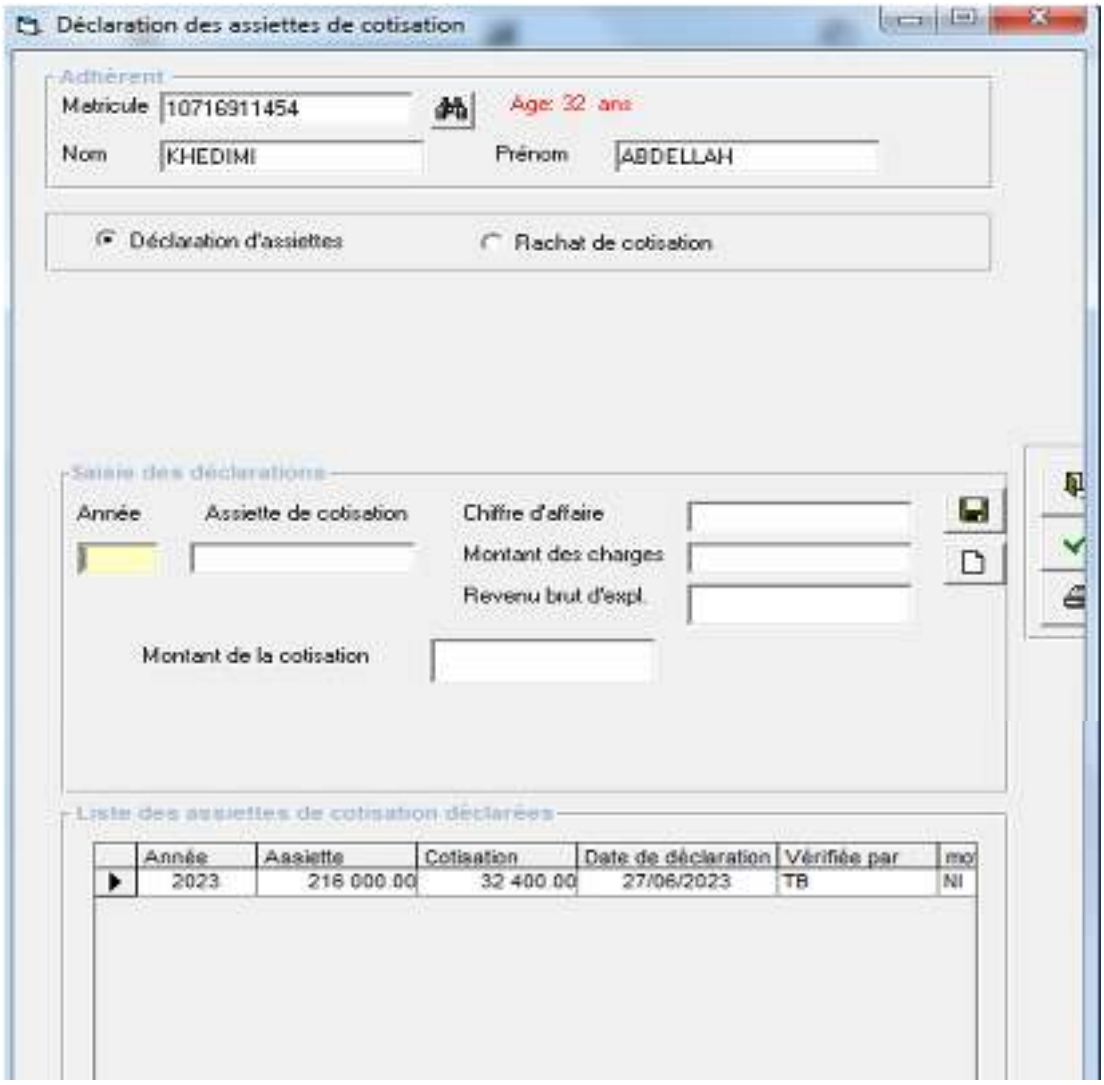

Figure 29 : Déclaration des assiettes de cotisation

Source : Service de recouvrement

La déclaration d'assiette des cotisations est l'assiette des salaires soumis aux cotisations sociales. Elle est constituée de l'ensemble des éléments du salaire et indemnités perçus durant la période travaillée, à l'exclusion des prestations à caractère exceptionnel et des indemnités liées aux conditions particulières de résidence et d'isolement, telles que définies par l'ordonnance 95-01 fixant l'assiette des cotisations et de prestations de sécurité sociale et explicitées par le décret 96-208 fixant les modalités d'application de l'article 1er de l'ordonnance 95-01.

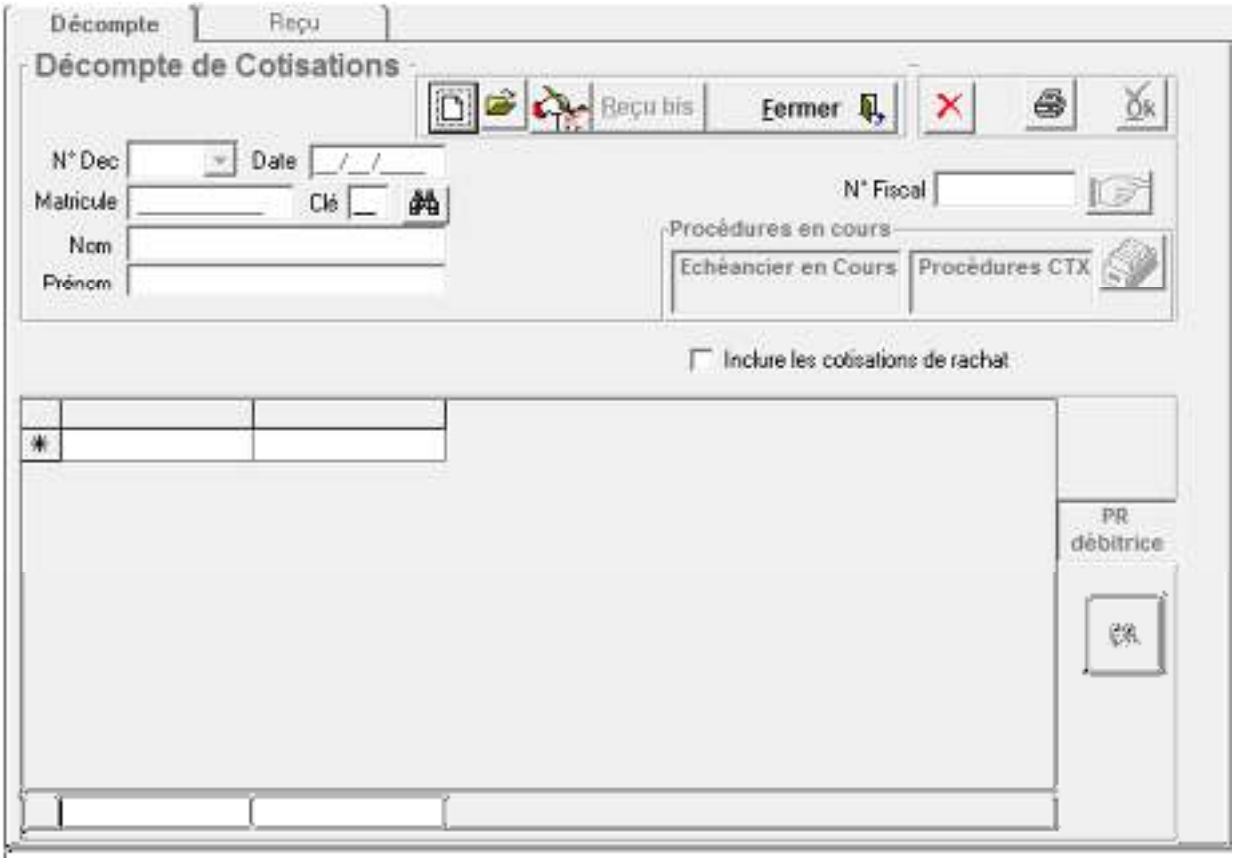

Figure : 30 Le décompte

Un décompte final des cotisations sociales est la différence entre les cotisations provisoires et les cotisations définitives. Votre fonds d'assurance sociale calcule le montant de vos cotisations définitives sur la base de vos revenus annuels réels. Le montant de vos cotisations provisoires est calculé en fonction de vos revenus des trois dernières années.

Le système de cotisations actuel des indépendants est entré en vigueur en 2015. Jusqu'en 2014, vous payiez vos cotisations sociales en fonction des revenus professionnels de trois ans auparavant. Ces cotisations ne pouvaient pas être adaptées ou recalculées.

Caisse Nationale de Sécurité Sociale des Non Salariés

ETAT DE DECOMPTE N° 35 102

Matricule: 10716911454 / 52 Classe : Non agricole

Nom: KHEDIMI Date : 10/07/2023

Prénom: ABDELLAH

Adresse : CITE LES FRERES KELOUAZE N 11 LES EUCALYPTUS

Période	Nature	Amiette	Montant facturé	Montant encaissé
PR 10722302423	R03	0,00	5 000,00	5 000,00
		TOTAL:	5 000,00 DA	5 000,00 DA

La somme a payer est: cinq mille Dinars Algeriens zéro centimes

LE LIQUIDATEUR LE VERIFICATEUR LE CAISSIER

Figure 31 : Relevé de compte

Source : Service de recouvrement

8.2. Plateforme assurances sociales [37]

Il trait 3 taches essentials sont comme suite:

8.2.1. Les gros risques :

8.2.1.1. Définition :

Le handicap peut être défini par la loi comme une condition médicale affectant la santé - qu'elle soit mentale ou physique - du travailleur, qui le rend complètement et définitivement incapable d'effectuer un travail.

[37] Service de prestations CASNOS

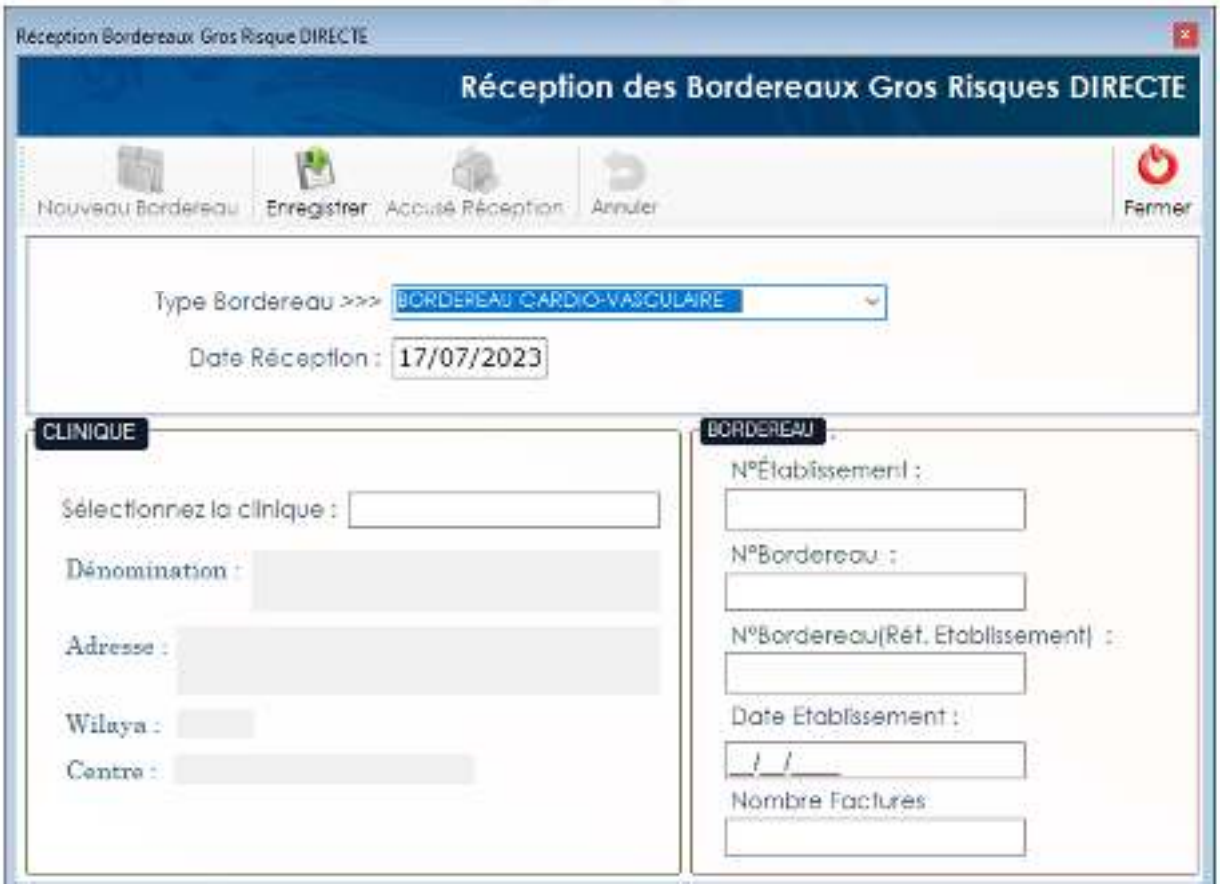

Figure 32 : Reception Borderaux Risque Directe

Source : Service de prestations

Dans le cas où cette invalidité survient et est prouvée selon les modalités légales, la personne handicapée assurée aura droit aux prestations de l'assurance invalidité après un délai de (6) mois à compter de la date du premier examen médical de la maladie. ou accident ayant causé l'invalidité, et a donc droit à bénéficier d'une pension d'invalidité de 80% ou 80% + 40%, selon l'état d'invalidité, du revenu annuel soumis à cotisation, à compter du premier jour de le septième mois à compter de la date du premier examen médical, conformément aux articles 4,5,6 du décret 35/85 du 2/1985. /09 .

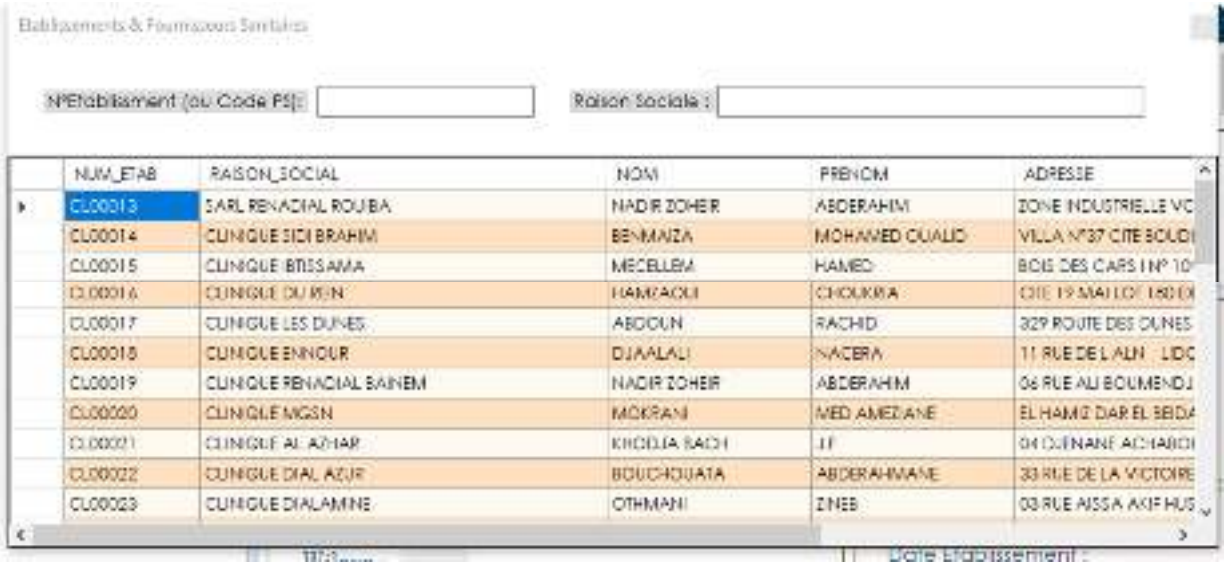

Figure 33 : Etablissements & Fournisseurs Sanitaire

8.2.1.2. Conditions d'indemnisation :

- Cette invalidité doit être totale et définitive
- La personne handicapée doit être en dessous de l'âge de la retraite
- Etre inscrit depuis au moins un an à compter de la date du premier examen médical
- Il doit être innocent de toute responsabilité envers le Fonds

A noter que le décret 35/85 mentionné ci-dessus classe le déficit en deux categories:

Cas 1- Lorsque la personne handicapée n'a pas besoin de l'aide d'autrui .

Cas 2- Lorsque la personne handicapée se trouve dans un état où elle a besoin de l'aide d'autrui

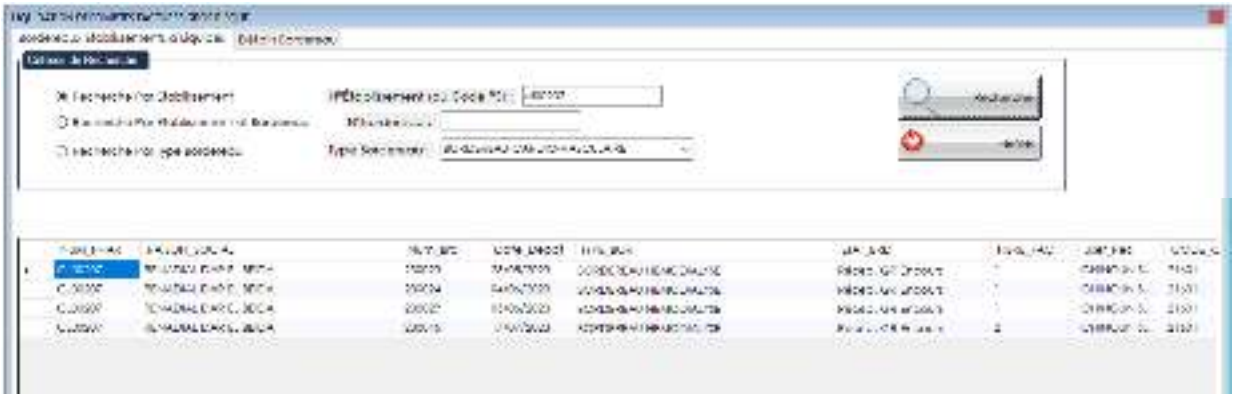

Figure 34 : Liquidation décompte Facture Gros Risque

8.2.1.3. La liquidation:

C'est la deuxième étape après réception des fichiers

L'agent chargé de liquider le dossier doit s'assurer que le dossier est conforme aux conditions .

Déterminé par la loi et la réglementation

Notamment la liste des médicaments non remboursables exclus par l'arrêté ministériel conjoint du 01/05/31, qui précise la liste des produits pharmaceutiques indemnisables par les caisses de sécurité sociale.

Cette liste est considérée comme le principal obstacle au travail du liquidateur car elle n'aborde pas la classification.

Médicaments selon une méthode dont dispose le liquidateur, c'est-à-dire (alphabétique) et la classification suivie (code de dénomination international) dans la liste, dont peuvent bénéficier les pharmaciens spécialisés.

Dans certains cas, le liquidateur doit assister l'ensemble de la liste, en plus de l'instabilité de cette liste, car elle est susceptible de changer de jour en jour.

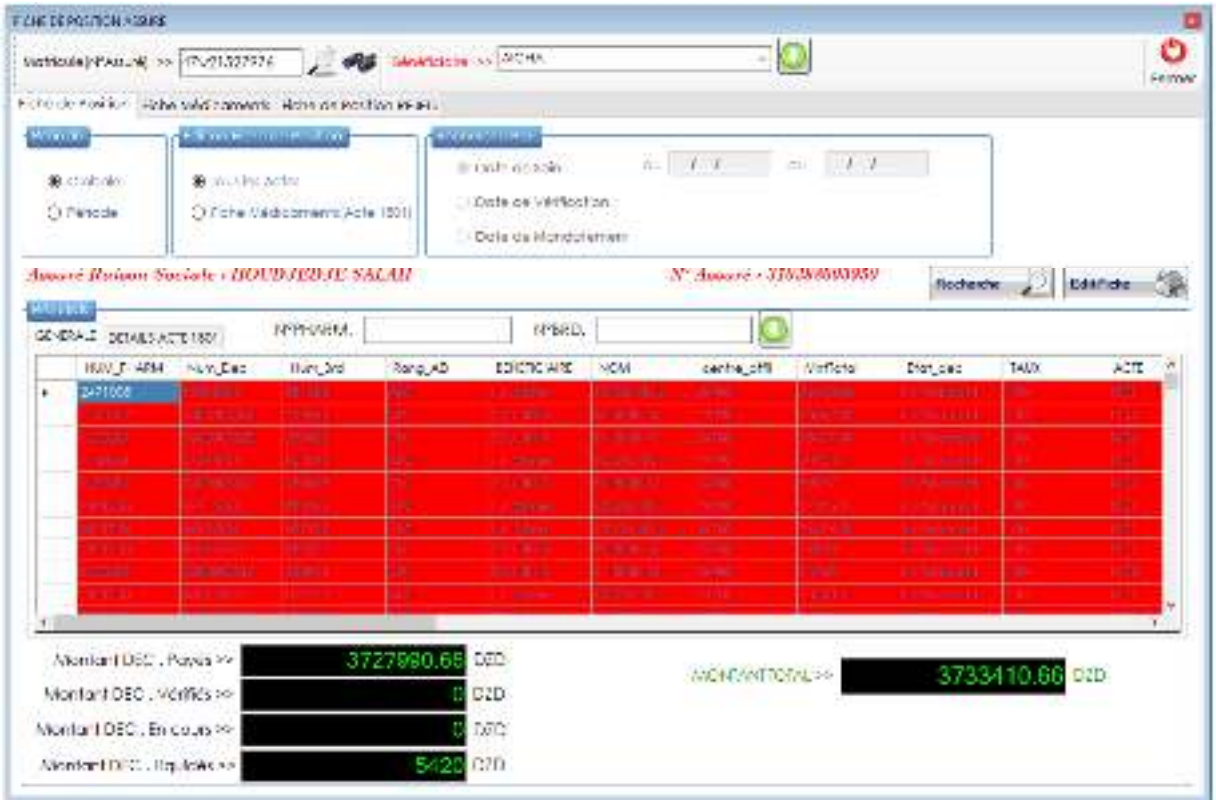

Figure 35 : Fiche de position assuré

Ainsi, nous voyons la nécessité de trouver une manière de classer les médicaments non remboursables, étant donné que leur nombre est bien inférieur à celui des médicaments indemnisables, et que la tâche de suivi soit confiée à l'un des médecins contrôleurs employés par l'agence, même si le processus relève des compétences de la Direction Centrale des Impôts, puisqu'elle est le superviseur général du processus d'orientation et de contrôle conformément au décret. Créateur de la Caisse de Sécurité Sociale pour les non-salariés, et ce, en l'absence de l'utilisation d'un dispositif d'information automatisé qui facilite le processus.

8.2.1.4. Imprimer LA SAISIE

Il s'agit de la troisième étape du dossier après réception et liquidation, où il est transféré pour enregistrer les données enregistrées sur la fiche de liquidation vers le dispositif d'information automatisé, qui complète le processus sous deux formes.

- Un tableau qui comprend le numéro, le nom, l'adresse et le montant de l'indemnisation de l'assureur

- Relevé de compte de rémunération

Il est à noter que ce processus est réalisé dans les délais malgré les dysfonctionnements qui surviennent constamment au niveau de l'imprimante.

- Les assistants doivent être formés pour mieux contrôler le système multimédia automatisé .

8.2.1.5. Verification:

Les taches du liquidateur adjoint viennent directement après le processus d'impression, puisqu'il imprime le décompte de rémunération et que le travail du commissaire aux comptes se concentre sur deux aspects.

- Suivi du liquidateur en termes d'adéquation de l'ordonnance et de la feuille de maladie avec le système d'indemnisation
- Suivi du travail d'impression avec le contenu de la carte filtre
- Suivi des erreurs typographiques, telles que le relevé de compte de compensation, pouvant survenir par l'assistant travaillant sur la machine à imprimer LA SAISIE

Surtout du nom - adresse - montant

8.2.2. Les tiers payant :

Le tiers payant dispense l'assuré de l'avance des frais (totalité ou ticket modérateur/reste à charge) délivrés dans un établissement conventionné avec la CASNOS.

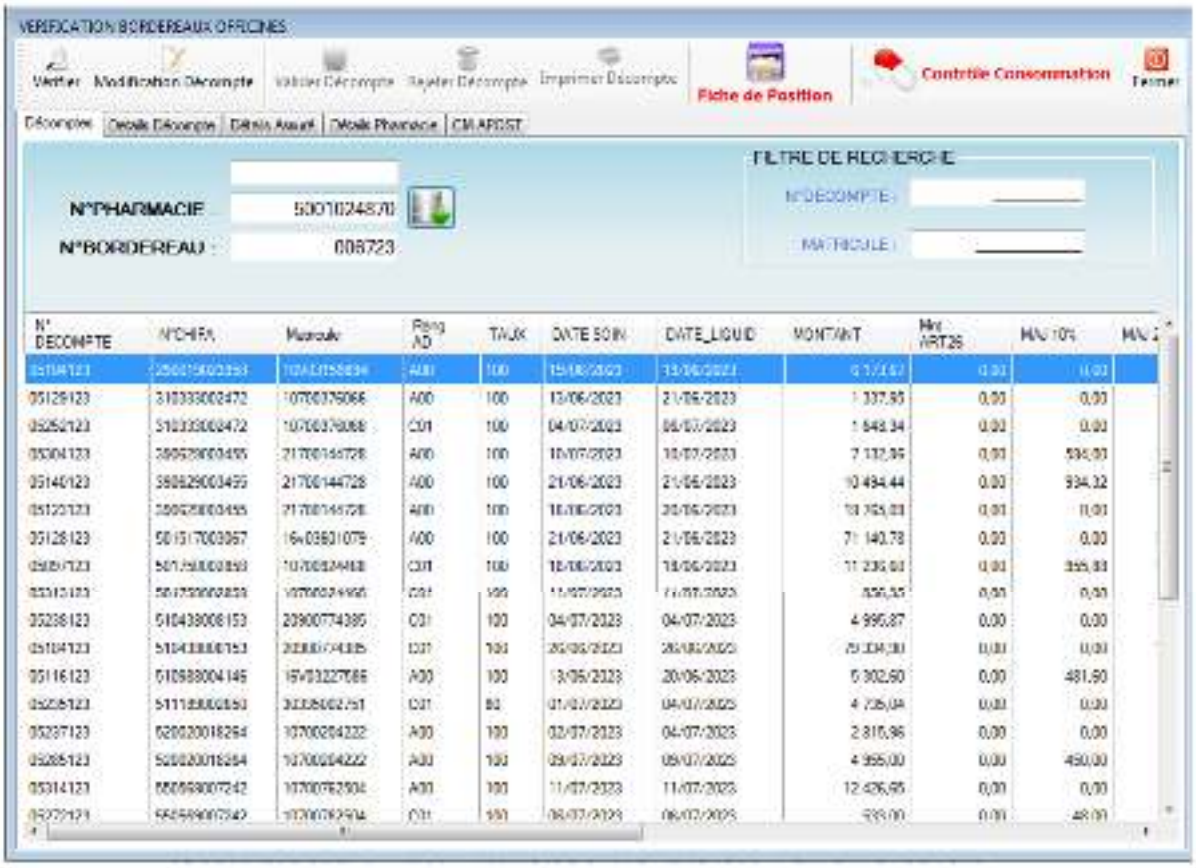

Figure 36 : Verification Borderaux Officines

Les taux de remboursement fixés actuellement par la réglementation en vigueur sont de 80% et de 100%

1/ Le remboursement au taux de 80%. Ce taux s'applique aux tarifs des

- Produits pharmaceutiques
- Cures thermales
- Actes professionnels des médecins, chirurgiens dentistes, pharmaciens et auxiliaires médicaux (fixé par l'arrêté interministériel du 04 juillet 1987)
- Journées d'hospitalisation, prestations d'hôtellerie et de restauration dans les cliniques privées et du tarif remboursable par la sécurité sociale (fixé par l'arrêté interministériel du 22 octobre 1988)

Figure 37 : Consommation de l'assuré

Le remboursement au taux de 100%. Le taux est porté à 100% des tarifs réglementaires dans les cas suivants

- Lorsque les frais engagés par l'assuré, le sont, à l'occasion de tout acte ou série d'actes affectés à la nomenclature des actes professionnels, d'un coefficient égal ou supérieur à K50.
- Lorsque le bénéficiaire est reconnu, après avis du contrôle médical, atteint de l'une des seize (16) affections de longue durée (article n°21 du décret 84/27 du 11 février 1984) ou de l'une des 10 affections prévues à l'article n°5 du même décret.
- Lorsque les frais sont engagés à l'occasion des fournitures de sang, de plasma et leurs dérivés.
- Pour le placement en couveuse des enfants prématurés.
- Lorsque les frais engagés concernent les actes et les produits relatifs à la contraception.
- Pour les ayants droit d'un travailleur décédé qui bénéficient du maintien des prestations parce qu'ils ont un revenu inférieur au salaire national minimum garanti (S.N.M.G.).
- Pour les titulaires d'un des avantages de sécurité sociale (Pension d'invalidité ou pension de retraite substituée à une pension d'invalidité, Pension de retraite, Allocation de retraite directe oude réversion) dont le montant est égal ou inférieur au salaire national minimum garanti (S.N.M.G), ainsi que leurs ayants droit.

- Pour les accouchements dystociques et suites de couches pathologiques.

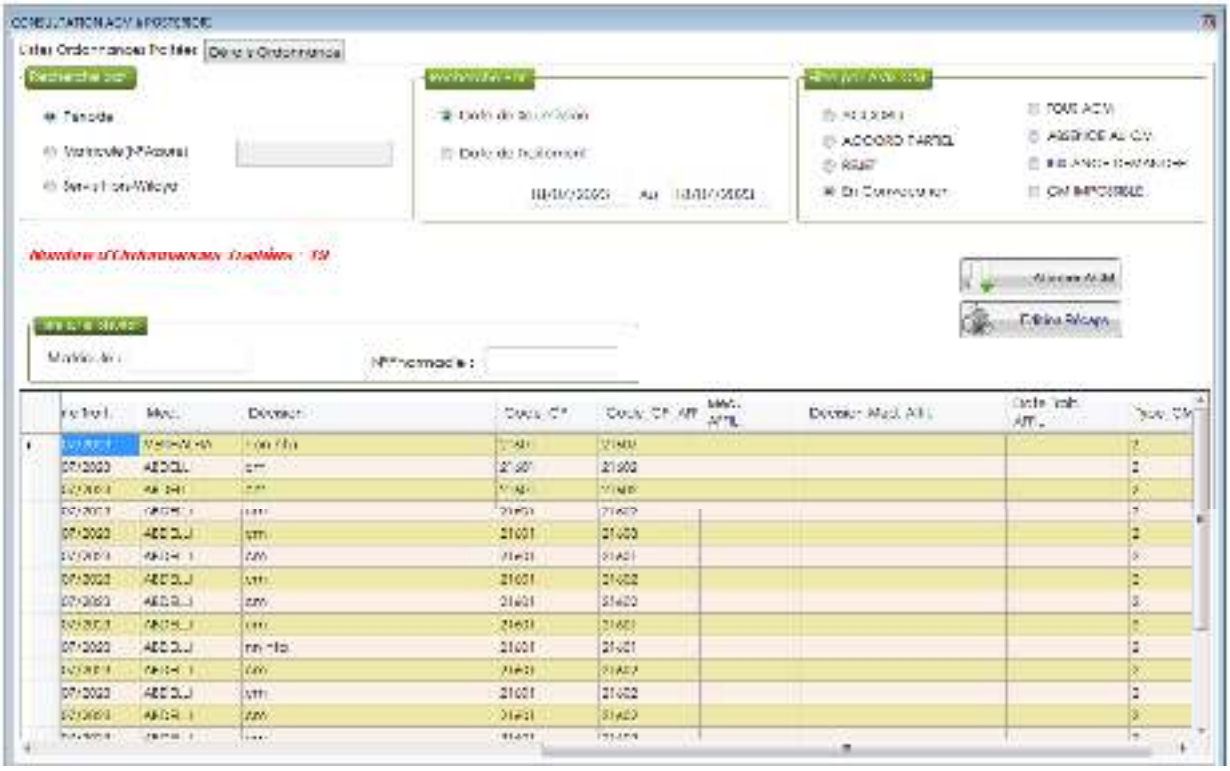

Figure 38 : Consultation a posteriori

Les prestations de l'assurance maternité sont prises en charge au taux de 100%, sur la base des tarifs fixés par voie réglementaire quand elles concernent

Les frais médicaux et pharmaceutiques.

Les frais d'hospitalisation de la mère et du nouveau-né pendant une durée maximale de huit (08) jours.

Le taux susvisé, c'est à dire 100%, peut être ramené à 80% si l'assuré social ne respecte pas certaines dispositions qui sont L'assuré social doit notifier à l'organisme de sécurité sociale (CASNOS) l'état de grossesse de son épouse par un document justificatif au moins six(06) mois avant la date présumé de l'accouchement, même procédure quand il s'agit d'une travailleuse non-salariés.

La future maman est tenue de se conformer à certains examens prénatals et postnatals qui sont

- un examen clinique complet avant le fin du 3éme mois de grossesse

- un examen obstétrical au cours du 6éme mois de grossesse
- deux examens gynécologiques : l'un quatre(04) semaines, au plus tôt, avant l'accouchement, et l'autre huit (08) semaines, au plus tard, après l'accouchement.

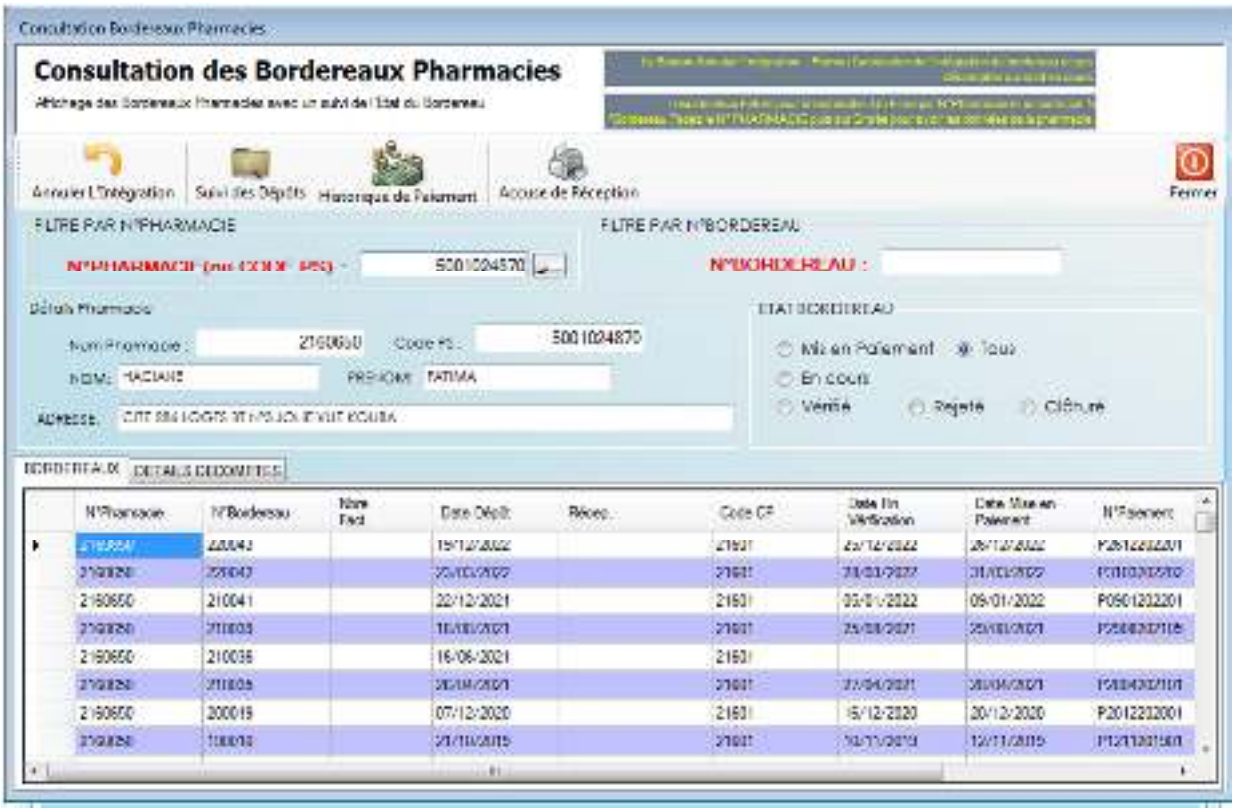

Figure 39 : Consultation Borderaux Farmacies

Le montant annuel de la pension d'invalidité est égal à 80% du revenu annuel soumis à cotisation.

Ce dernier est constitué par le revenu annuel imposable au titre de l'impôt sur le revenu et dans la limite d'un plafond annuel de huit (08) fois le montant du salaire national minimum garanti (SNMG) (c'est à dire (10 000*8)*12 = 80 000 DA/mois).

Par ailleurs, il faut signaler que la pension d'invalidité ne doit pas être inférieure à un minimum de 75% du salaire national minimum garanti(SNMG) (Conf. Art 1 du décret législatif n°94-04 du 11 avril 1994)

Ce minimum est : 10 000,00 * 12 * 75% = 7 500,00 DA/mois.

Enfin, il faut noter que lorsque l'invalide est dans l'obligation d'avoir recours à l'assistance d'une tierce personne, le montant de la pension d'invalidité est majoré de 40%.

Figure 40 : Premaration Paiement Officines Pharmaceutiques

Le montant de la pension de retraite ou de l'allocation de retraite s'établit de la même manière.
La différence entre ces deux prestations est que le revenu minimum n'est pas applicable sur l'allocation de retraite.
Le montant de la pension de retraite ou l'allocation de retraite est fonction de trois paramètres qui sont
Le nombre d'années de cotisation
Le pourcentage par année liquidable
L'assiette devant servir de base au calcul de la pension
Pour chaque année de cotisation validée, il est compté 2,5% de l'assiette devant servir de base pour le calcul de la pension. Le pourcentage ne peut dépasser 80%.
L'assiette servant de base au calcul de la pension de retraite est constitué par la moyenne, calculée sur les 10 meilleures années, des revenus annuels soumis à cotisation. (Cf. article 10 du décret n°85-35 du 09 février 1985)

Figure 41 : Etats Comptables Et Statistiques De Paiements

8.2.3. La carte chifa :

La carte CHIFA est la carte d'assurance maladie de la sécurité sociale en Algérie. Une carte à puce au format carte de crédit qui permet à son propriétaire et ses ayants droit de bénéficier des prestations de sécurité sociale concernant les dépenses de santé.

Figure 42 : Platforme Assurance Sociale

Quelles sont les données insérées dans la carte CHIFA ?

Conformément aux dispositions de l'**article 8 du décret exécutif n°10-116** modifiés par l'**article 2 du décret exécutif n°18-228**, la carte CHIFA familiale ou d'ayant(s) droit est composée des données électronique suivantes :

Les données administratives concernant l'assuré social et ses ayants droit portés sur la carte

Les données relatives à l'affiliation à la sécurité sociale de l'assuré social et, le cas échéant, les données relatives à son adhésion à une mutuelle sociale ;

Les droits aux prestations servies à l'assuré social par l'organisme de sécurité sociale ainsi qu'à ses ayants droit et, le cas échéant, le droit aux prestations servies par la mutuelle sociale ;

Les données à caractère médical de l'assuré social, du
ou des bénéficiaires selon le type de carte familiale ou d'ayant(s) droit ;

L'ensemble des prestations servies par l'organisme de sécurité sociale d'affiliation, à l'assuré social titulaire de la carte et/ou à ses ayants droit portés sur la carte et, le cas échéant, l'ensemble des prestations servies par la mutuelle sociale ;

Les données relatives à l'utilisation et à la sécurisation de la carte.

Figure 43 : Reception Dossier Assuré

Comment obtenir la carte CHIFA ?

La carte CHIFA est délivrée gratuitement à tout assuré social affilié à un organisme de sécurité sociale.

L'assuré doit, donc se déplacer au niveau du centre de paiement d'affiliation muni du dossier suivant :

- Photo d'identité sur fond clair
- Photocopie de la carte d'identité
- Extrait de naissance n°12
- Photocopie de la carte de groupage sanguin

Il faudra bien évidemment attendre une (01) semaine afin de la récupérer.

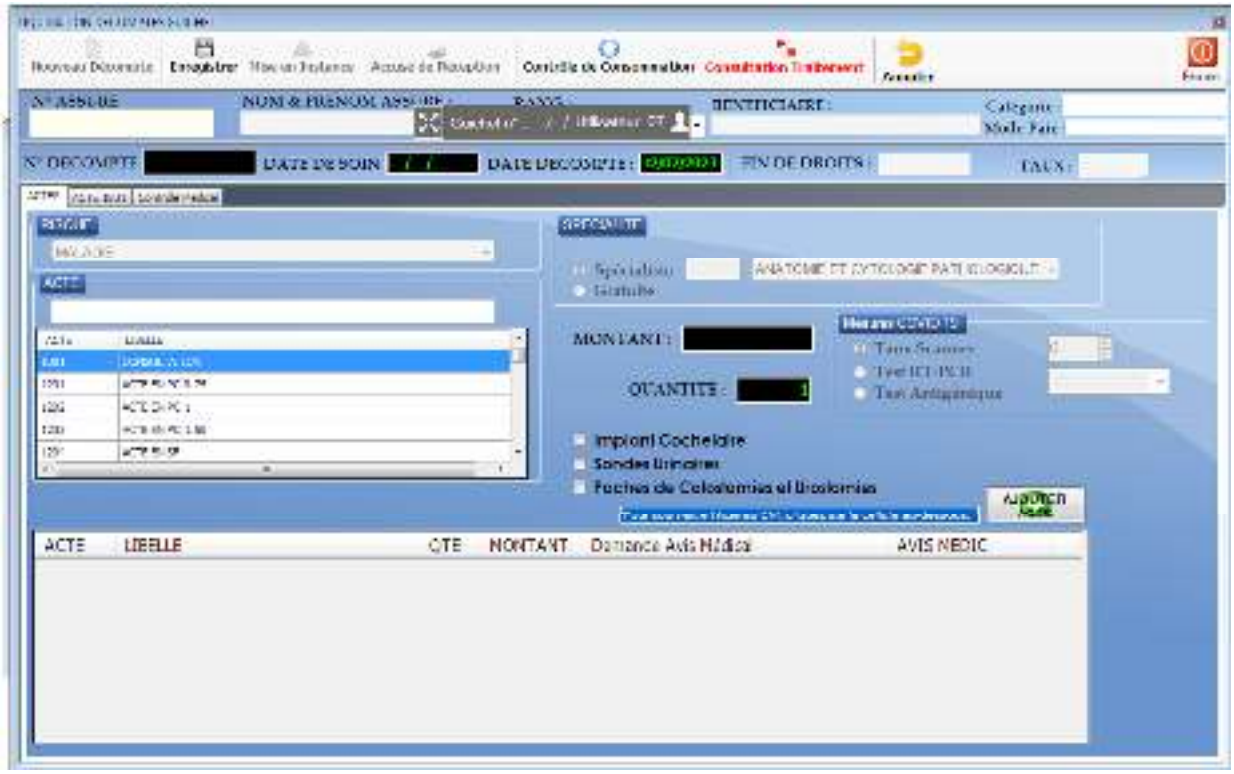

Figure 44 : Liquidation Dossier Guichet

Que couvre la carte CHIFA ?

La carte CHIFA couvre les prestations ; Médicales, Chirurgicales, d'hospitalisation, actes médicaux de diagnostic et thérapeutiques, y compris les explorations biologiques, d'appareillages et de prothèse, de rééducation fonctionnelle et réadaptation professionnelle, de soins et de prothèses dentaires et d'orthopédie maxillo-faciale, d'optique médicale, de cures thermales ou spécialisées.

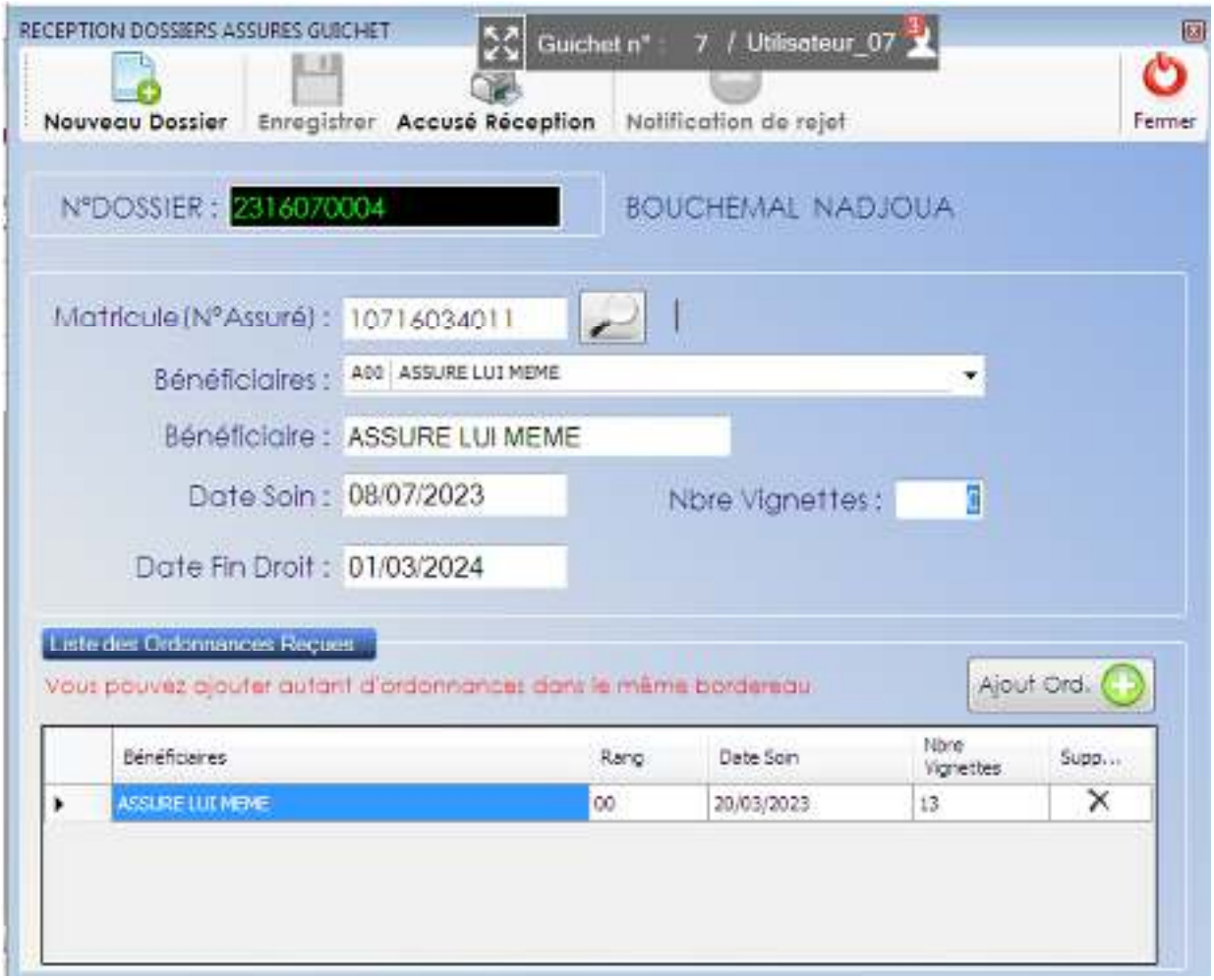

Figure 45 : Liste des Orodonnances Recues

8.3. Systéme de retraitre [38]

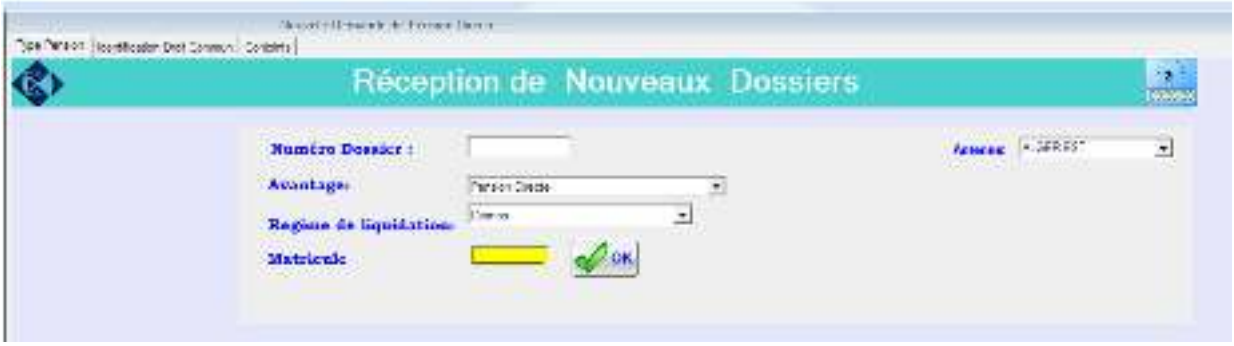

Figure 46 : Reception de Nouveaux Dossiers

[38] Service de retraite CASNOS

Un système de retraite est source de redistribution intragénérationnelle si la répartition primaire des revenus (sans régime de retraite) sur l'ensemble du cycle de vie diffère de la répartition secondaire des revenus (avec un régime de retraite) pour une génération donnée (Walraet et Vincent, 2003).

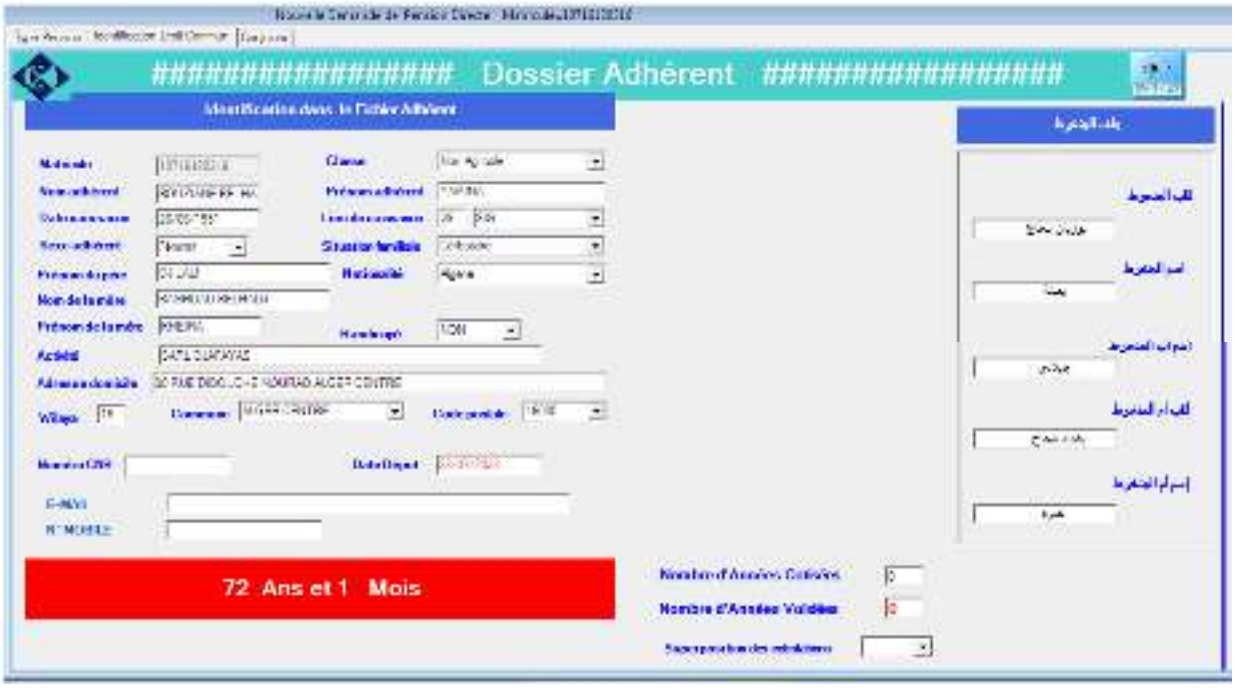

Figure 47 : Nouvelle Delande de Pension Directe

Le système de retraite algérien est un système par répartition, contributif et à prestations définies. Deux régimes le constituent : l'un pour les salariés, géré par la Caisse nationale des retraites (CNR), l'autre pour les non-salariés, géré par la Caisse nationale des non-salariés (Casnos). Dans la suite de cet article, pour en simplifier la lecture, nous ne désignerons par « système de retraite algérien » que le régime des salariés. L'intérêt que nous portons à ce dernier est justifié par le nombre de retraités couverts par ce régime par rapport au régime des non-salariés : 1253839 pour le premier versus 122198 pour le second, en 2000 (Office national des statistiques [ONS], 2003)

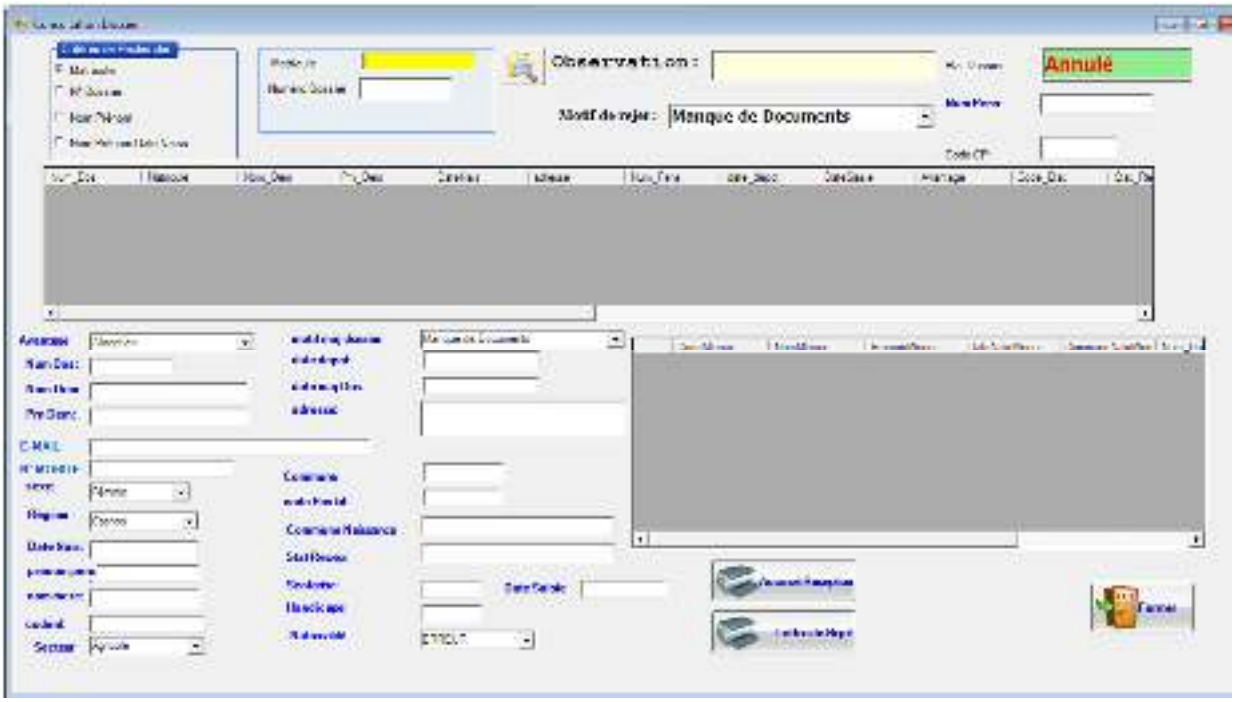

Figure 48 : Consultation Dossier

L'âge légal de départ à la retraite est de 60 ans pour les hommes et 55 ans pour les femmes, avec une réduction d'un an par enfant pour les femmes qui ont élevé un ou plusieurs enfants pendant au moins neuf ans, dans la limite de trois enfants. Comme dans tout régime à prestations définies, le montant de la pension principale dépend du niveau du salaire de référence et du nombre d'années d'activités professionnelles validées. Le salaire de référence est le salaire moyen des cinq années précédant le départ à la retraite, ou, si cela se révèle plus favorable, la moyenne des salaires des cinq meilleures années de la carrière professionnelle.

Figure 49 : Liquidation d'une Pension Directe

Le financement du système de retraite algérien repose sur une base assurantielle et contributive. Les recettes proviennent des cotisations à la charge des employeurs et des salariés, des revenus du Fonds national de réserve des retraites (FNRR) [1][1]) (Le Fonds national de réserve) placés et du budget de l'État. En effet, afin d'assurer la cohésion sociale et de maintenir l'équilibre financier de la CNR, le budget social de l'État prend en charge certaines prestations non contributives du système de retraite, telles que les compléments différentiels, les indemnités complémentaires, les majorations exceptionnelles et les pensions des Moudjahidines (encadré 1). Ainsi, l'État intervient pour assurer la justice sociale via la prise en charge des avantages non contributifs qui s'ajoutent aux avantages contributifs.

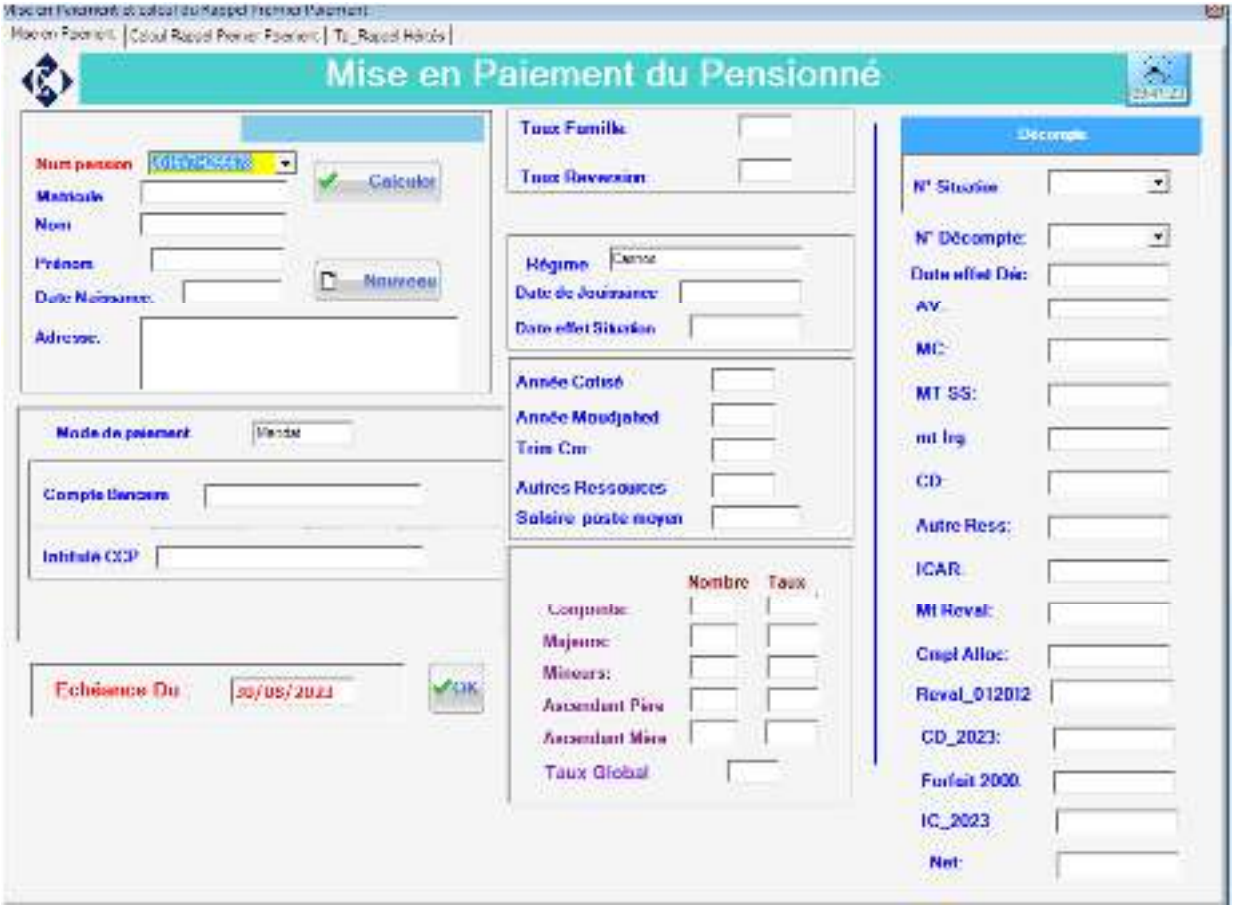

Figure 50 : *Mise en paiement et Calcul du Rappel Premier Paiement*

8.3.1 Modes de redistribution intergénérationnelle

D'une manière très simplifiée, « un système de retraite est qualifié de redistributif quand il corrige la répartition initiale inégalitaire des revenus primaires et assure soit les mêmes prestations à tous, indépendamment des revenus, soit des prestations plus importantes pour ceux qui ont les revenus les plus faibles » (Legros, 1994).

L'inégalité mesure une différence relative de situation entre individus, au regard soit du revenu, soit de l'accès à certaines prestations. Pour le cas de l'Algérie, nous distinguons deux types d'inégalités : l'une est relative à la couverture partielle de la population, l'autre se situe parmi les retraités couverts (Dupuis, El Moudden et Petron, 2009). Certes, l'inégalité la plus marquante est celle qui oppose les personnes âgées couvertes par un système de retraite aux personnes âgées non couvertes. Toutefois, dans ce travail, nous aborderons l'inégalité à travers les disparités entre les montants des pensions.

Section 3: La securité des systémes d'informations pour la CASNOS [39]

1. Qu'est-ce que la sécurité des systèmes d'information ?

L'informatique n'étant finalement qu'un moyen de faciliter la gestion de l'information, il serait donc réducteur de considérer que protéger ses outils, c'est protéger l'information de l'entreprise. La sécurité des systèmes d'information (SSI) prend en compte tous les éléments qui composent le SI : les utilisateurs, les procédures et les outils.

Protéger son SI, c'est donc aussi sensibiliser les utilisateurs à la sécurité ou revoir certaines procédures comportant des risques pour le patrimoine informationnel de l'entreprise.

2. Comment identifier ce qui doit être protégé ?

La première étape est de réaliser un état des lieux afin d'avoir une vision d'ensemble de son système d'information.

Il n'est pas toujours facile pour un dirigeant de mesurer l'étendue de l'information détenue par son entreprise car elle n'est généralement pas stockée dans un lieu unique.

Dans un premier temps, commencez par recenser :

- Les ressources internes de votre entreprise : messagerie électronique (emails, contacts, agenda), données stratégiques, fichier clients, données techniques…
- Les ressources de l'entreprise exploitées ou détenues par un prestataire extérieur ou un tiers.
- Les ressources appartenant à un prestataire extérieur exploitées par lui au profit de votre entreprise.

3. Hiérarchiser la valeur des informations :

Pour définir le degré de valeur ajoutée de chaque type de données, hiérarchisez la valeur des informations selon l'importance de leur disponibilité et de leur intégrité.

Attribuez ensuite des droits d'accès aux documents à l'aide de profils utilisateurs selon leur degré de responsabilité dans l'entreprise. Il est préférable de désigner une personne responsable pour ce type d'activité.

[39] Service informatique CASNOS

Pour vous aider dans la démarche de classification de vos données, vous pouvez vous inspirer librement du tableau ci-dessous. En voici la légende :

Information sensible : information susceptible de causer des préjudices à l'entreprise si elle est révélée à des personnes mal intentionnées pouvant entraîner la perte d'un avantage compétitif ou une dégradation du niveau de sécurité.

Information stratégique : information essentielle et critique contenant la valeur ajoutée de l'entreprise (savoir-faire, procédures, méthodes de fabrication…).

3. Evaluer les risques :

la phase d'évaluation des risques internes et externes permet d'identifier les différentes failles, d'estimer leur probabilité et d'étudier leur impact en estimant le coût des dommages qu'elles causeraient.

3.1 Quelles sont les menaces ?

Une menace est une action susceptible de nuire et de causer des dommages à un système d'information ou à une entreprise. Elle peut être d'origine humaine (maladresse, attaque) ou technique (panne) et être interne ou externe à l'entreprise.

3.2 Quels impacts pour l'entreprise ?

L'analyse d'impact consiste à mesurer les conséquences d'un risque qui se matérialise.

	3 : secret	2 : confidentiel	1 : diffusion contrôlée
Préjudice potentiel	Préjudice grave Séquelles compromettant l'action à court et moyen terme	Préjudice faible Perturbation ponctuelles	Préjudice faible Perturbation ponctuelles
Risques tolérés	Aucun risque même résiduel n'est acceptable	Des risques très limités peuvent être pris	Des risques sont pris en connaissance de cause
Protection	Recherche d'une protection maximale	Prise en compte de la notion de probabilité d'occurrence	La fréquence et le coût du préjudice potentiel déterminent les mesures prises

Figure 51 : Tableau de classification des risques selon le degré d'importance des informations

4. Bâtir une politique de sécurité adéquate :

4.1 Les grands principes :

La SSI repose sur trois finalités :

- L'intégrité du SI : s'assurer de son bon fonctionnement, de l'exactitude des données et de leur intégrité.
- La confidentialité SI : s'assurer que seules les personnes autorisées ont accès aux données.
- Les différentes ressources (ordinateurs, réseaux, périphériques, applications) sont accessibles au moment voulu par les personnes autorisées.

En fonction de ces objectifs, la politique de sécurité de l'entreprise va se décliner de trois man .

Stratégique : définition des objectifs globaux de sécurité, définition qui découle du travail d'état des lieux, de hiérarchisation des données selon leur importance stratégique et d'analyse des risques.

Organisationnel : plan de secours, charte utilisateur, définition du rôle de chaque membre du personnel, sessions de sensibilisation des collaborateurs à la SSI.

Technique : mise en place des moyens de protection (antivirus, mot de passe…).

Sécuriser son SI :

ll s'agit de mettre en place des mesures préventives et curatives.

Certaines reposent sur des outils et d'autres sur le comportement des utilisateurs.

Mais avant de mettre en place ces mesures, l'entreprise doit d'abord statuer sur 2 questions :

- Quelle est la quantité maximale d'informations qui peut être perdue sans compromettre l'activité de l'entreprise ?
- Quel est le délai maximum de reprise d'activité acceptable sans menacer le fonctionnement de la société ?

La réponse à ces questions va permettre d'évaluer le niveau de sécurité que l'entreprise devra mettre en place et de déterminer les informations qui devront être protégées et rétablies en priorité en cas de sinistre pour générer un minimum de pertes, y compris financières.

- **Les mesures préventives** Elles permettent d'éviter une interruption de l'activité.

Voici les principaux points de vigilance :

- **Plan de sauvegarde :** il s'agit de déterminer la fréquence et le type de sauvegarde (complète, différentielle, incrémentale) pour chaque catégorie d'information (basique, sensible, stratégique).
- **Sécurité logique :** il convient de mettre en place des outils de protection de base (anti-virus, firewall, anti-spam) et de les mettre à jour. A cela peuvent s'ajouter des contrôles d'accès aux données par mot de passe ou certificat électronique.
- **Sécurité physique :** il s'agit de la sécurité des locaux. Une attention particulière doit être portée à la sécurité du serveur de l'entreprise.
- **Le facteur humain :** la sécurité des systèmes d'information n'est pas qu'une affaire d'outils mais dépend aussi et surtout d'une information régulière aux utilisateurs de l'informatique dans l'entreprise. Des règles élémentaires (comme ne pas noter son mot de passe sur un papier) doivent être ainsi rappelées.

- **Mesures curatives :** Ces mesures sont nécessaires car aucune mesure préventive n'est efficace à 100%. Elles sont mises en œuvre lorsqu'un sinistre survient :

- Restauration des dernières sauvegardes.

- Redémarrage des applications.

- Redémarrage des machines (ordinateurs…).

5. Quels outils utiliser pour une protection minimum du SI ?

Les outils de protection de base :

Il est impératif qu'au sein de votre entreprise, chaque poste de travail et/ou le serveur soit protégé par un antivirus et un pare-feu (firewall) mis à jour.

5.1. L'antivirus :

5.1.1 Qu'est-ce que c'est ?

Il s'agit d'un logiciel permettant de protéger son poste informatique ou son système contre les infections informatiques.

Ce logiciel surveille et analyse régulièrement l'ensemble des fichiers puis filtre les contenus suspects.

Une fois l'anomalie détectée, il vous en informe et la détruit. La plupart des logiciels antivirus intègrent également une protection antispam qui permet d'analyser l'ensemble des messages entrants avant qu'ils ne soient délivrés au destinataire.

5.1.2 Comment fonctionne-t-il ?

L'antivirus fonctionne à partir d'une base d'empreintes de virus connus ou d'un système d'intelligence artificielle détectant les anomalies. C'est pourquoi, pour une efficacité optimale, il est indispensable de le mettre à jour régulièrement (aussi bien la base d'empreintes que l'application elle-même).

5.2 Le pare-feu

5.2.1 Qu'est-ce que c'est ?

Un pare-feu ou firewall (en anglais) désigne un dispositif capable de bloquer les virus et d'éviter la fuite d'informations vers l'extérieur. Lorsque des données sont transmises entre ordinateurs via Internet, les informations entrent et sortent par des portes virtuelles appelées « ports ». Chaque ordinateur dispose de 65 536 ports.

Ces « entrées » sont autant de possibilités de pénétrer dans le système d'information de l'entreprise. Si bien qu'en l'absence de pare-feu, des pirates informatiques ont tout loisir d'infecter ou de détruire les données d'un ordinateur (virus, vers) ou de récupérer des informations via un cheval de Troie.

5.2.2 Comment fonctionne-t-il ?

Un pare-feu joue un rôle de douanier vis-à-vis des ports. Il contrôle les flux de données entrant et sortant de l'ordinateur ou du réseau de l'entreprise. Il est très fréquent qu'un logiciel professionnel ait besoin d'accéder à un serveur extérieur à l'entreprise pour effectuer des mises à jour. Il lui faut alors communiquer par un canal spécifique (port de communication), à la fois pour émettre des données (port sortant) mais aussi pour en recevoir (port entrant). Les règles de

filtrages doivent donc autoriser ces ports de communication pour permettre au logiciel de télécharger la mise à jour.

Il existe deux catégories de pare-feu :

- Le pare-feu personnel est un logiciel installé sur les postes informatiques permettant de protéger uniquement le système sur lequel il est installé. Windows, par exemple, en comporte un par défaut.
- Le pare-feu réseau se présente sous forme de boîtier placé entre un accès externe et un réseau d'entreprise.

6. Sécuriser les échanges de données

6.1 Qu'est-ce que c'est ?

Le certificat électronique est une carte d'identité numérique permettant de garantir l'intégrité des informations et documents transmis et de s'assurer de l'identité de l'émetteur et du récepteur de ces données. Il contient des informations sures :

- L'autorité de certification qui a émis le certificat
- Le certificat électronique (validité, longueur des clefs,)
- Le titulaire du certificat (nom, prénom, service, fonction) et son entreprise (dénomination, n° Siren).

6.2 Comment s'en procurer ?

Le certificat électronique est délivré pour une durée déterminée par une Autorité de Certification qui joue le rôle de Tiers de confiance. Cet organisme garantit l'identité de la personne et l'usage des clés par une personne qui en est la seule propriétaire. De plus, elle atteste de l'exactitude des informations contenues dans le certificat.

6.3 Comment ça marche ?

Lorsque les données transitent, elles sont cryptées. Le certificat électronique fonctionne selon un principe de clé : l'émetteur et le récepteur des données disposent chacun d'une clé publique , servant au chiffrement du message, et d'une clé privée , servant à déchiffrer le message.

Le certificat numérique consiste à déterminer si une clé publique appartient réellement à son détenteur supposé. Il peut être stocké sur un support logiciel ou matériel (une carte à puce à insérer dans un lecteur de carte ou une clé USB).

6.4 Ses usages

Le certificat électronique est de plus en plus utilisé, notamment dans le cadre des téléprocédures administratives (TéléTVA, télécarte grise…). Voici deux autres types d'usages en entreprise :

- **La signature électronique**

Elle possède la même valeur juridique et la même fonction qu'une signature manuscrite.
Une différence notable les distingue cependant : alors qu'une signature manuscrite peut être facilement imitée, une signature numérique est pratiquement infalsifiable.
La loi accorde d'ailleurs un statut particulier à la signature électronique.

- **Le VPN**

Un VPN (Virtual Private Network) permet d'accéder à la totalité des fichiers d'une entreprise en toute sécurité. Il donne accès au réseau local d'une entreprise à distance via une connexion Internet sécurisée.

Les données qui transitent sont chiffrées grâce à une technique de « tunnel » et donc inaccessibles aux autres internautes. Ce cryptage est rendu possible grâce à un certificat électronique. Celui-ci fonctionne comme un passeport. Il doit être présent à la fois du côté de l'ordinateur distant qui tente d'accéder aux fichiers de l'entreprise et du côté du serveur.

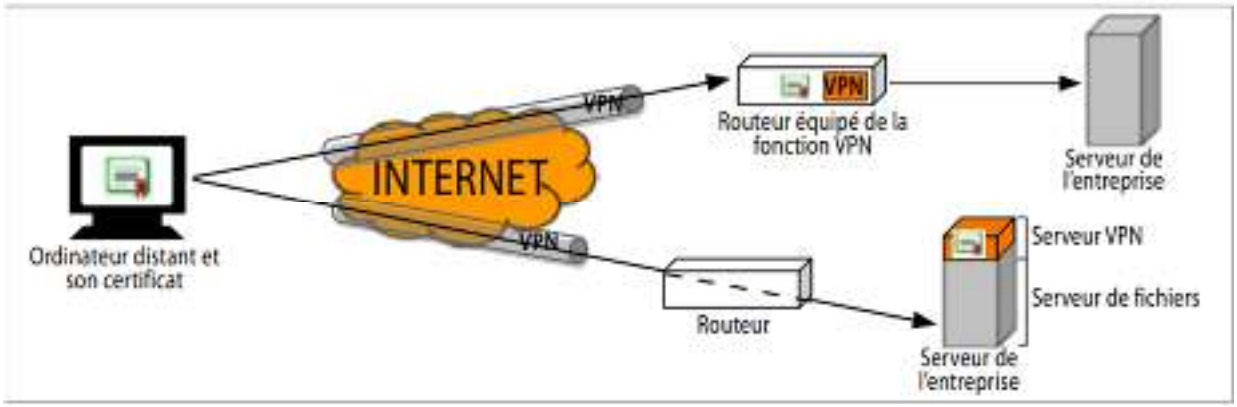

Figure 52 : Accès au serveur de fichiers à distance grâce à un VPN

7. Gérer le courrier électronique indésirable :

7.1 Le spam, qu'est-ce que c'est ?

7.1.1 Origine du mot

A l'origine, « SPAM » est la marque déposée d'une conserve de jambon épicée « SPiced hAM », consommée en très grande quantité par les américains lors de la seconde guerre mondiale et redevenue populaire grâce aux Monthy Pythons en 1970.

7.1.2 Principe

Le spam consiste à envoyer massivement des emails non sollicités à des fins marchandes (vente de médicaments par exemple) ou malveillantes (récupération d'adresse emails valides, propagation de virus). Ce type de courrier électronique n'est généralement pas ciblé mais envoyé à une multitude de destinataires par l'intermédiaire de serveurs automatisés.

7.2 Les impacts du spam

- La saturation du réseau ou des serveurs de messagerie de l'entreprise.
- Des risques de blocage de l'adresse IP de l'entreprise par les fournisseurs d'accès Internet si l'adresse de l'entreprise est usurpée par un spammeur.
- Le gaspillage de la bande passante et de l'espace de stockage des utilisateurs.
- La dégradation de l'image de l'entreprise si l'adresse de l'entreprise est usurpée par un spammeur.
- La perte de productivité des employés qui risquent de surcroit de passer à coté d'emails importants.

7.3 Comment se protéger contre le spam?

6.3.1 Eviter d'être spammé :

- Ne jamais répondre à un message dont l'objet ou l'expéditeur est douteux.
- Ne pas diffuser son adresse sur le web (dans des forums ou des sites par exemple).
- Créer une ou plusieurs « adresses poubelles » servant uniquement à vous inscrire ou vous identifier sur les sites jugés dignes de confiance.
- Sur son site Internet, crypter les adresses de la page contact.

7.3.2 Mettre en place un anti spam :

7.3.2.1 Les logiciels

Il existe différents types de logiciels anti-spam. Vous pouvez en choisir un seul ou en cumuler plusieurs. Pour les entreprises possédant moins de 500 postes informatiques, 3 types d'outils sont conseillés :

- ✓ **Les outils clients :** il s'agit de logiciels installés sur chaque poste informatique.
- ✓ **Les outils serveurs :** les messages reçus sont filtrés dès leur arrivée dans le serveur de messagerie avant d'être remis au destinataire.
- ✓ **Les solutions hébergées** : dans ce cas, l'analyse anti-spam intervient avant que le message n'arrive dans le serveur de messagerie.

7.3.2.2 Les méthodes de filtres anti-spam :

Ces logiciels utilisent une ou plusieurs des méthodes de filtrage suivantes.

- ✓ Le filtrage par mot clé permet d'effectuer un blocage des emails contenant certains mots répertoriés dans un dictionnaire de détection. Toutefois, il est très facile pour le spammeur de contourner cette technique.
- ✓ Le filtrage par analyse lexicale (bayésien) consiste à rechercher des mots clés associés à un système de pondération. Difficile à contourner, il tient compte de l'ensemble du message, est multilingue et utilise l'intelligence artificielle.
- ✓ Le filtrage heuristique consiste à analyser le contenu des messages en vérifiant la présence de forme et de code (HTML dans le corps du message, mots écrits uniquement avec des lettres majuscules ; mots clés correspondants à des produits souvent vantés au travers du Spam, très grand nombre de destinataires…)

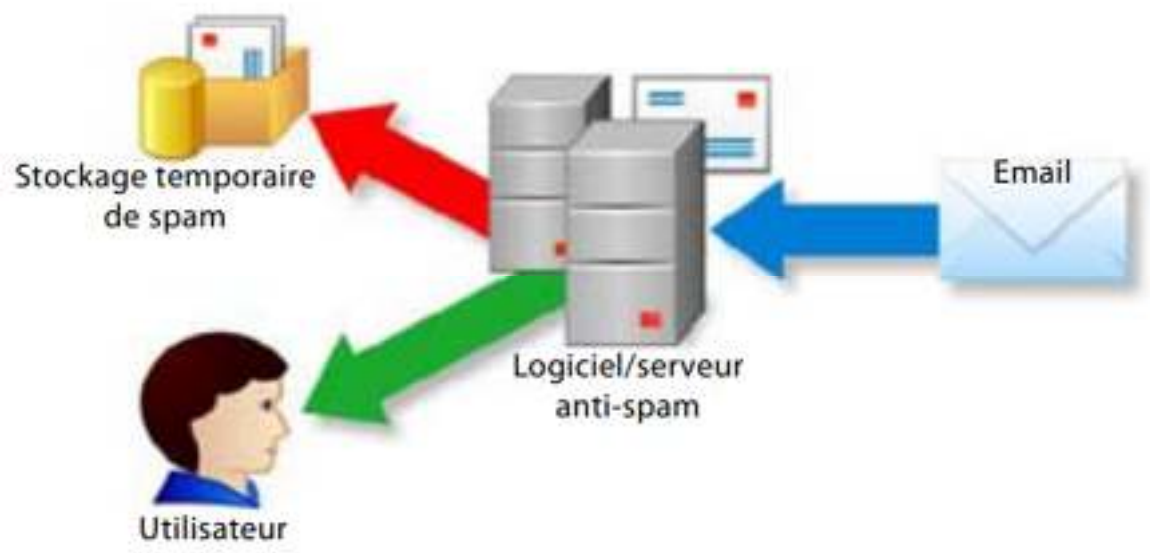

Figure 53 : *Principe de fonctionnement d'un logiciel anti-spam hébergé*

8. Comment sauvegarder vos données numériques ?

8.1 Etablir un état des lieux des données à sauvegarder :

il s'agit, dans un premier temps, de faire l'inventaire des données de l'entreprise : fichiers, base de données, emails, etc. Puis, les informations stratégiques devront être identifiées car une attention particulière devra leur être portée en matière de fréquence et de support de sauvegarde.

8.2 Choisir le type de sauvegarde

8.2.1 Sauvegarde complète

Elle permet de réaliser une copie conforme des données à sauvegarder sur un support de sauvegarde séparé.

8.2.2 Sauvegarde au fil de l'eau : sauvegarde incrémentale

Elle se limite uniquement aux informations modifiées ou ajoutées depuis la dernière sauvegarde .

8.2.3 Sauvegarde différentielle

Elle permet de sauvegarder toutes les informations modifiées ou ajoutées depuis la dernière sauvegarde complète.

8.3 Choisir la fréquence des sauvegardes :

- La périodicité et la durée des sauvegardes dépendent de plusieurs facteurs :
- Le volume de données.
- La vitesse d'évolution des données.
- La quantité d'information que l'on accepte de perdre.
- Eventuellement, la durée légale de conservation de l'information (ex : facture).

C'est pourquoi, selon les entreprises, la stratégie de sauvegarde sera différente.

Voici un exemple de stratégie de sauvegarde :

8.3.1 Fréquence de sauvegarde

• Une sauvegarde complète dans la nuit du vendredi au samedi pour ne pas gêner l'activité de l'entreprise.

• Une sauvegarde incrémentale les autres nuits.

• Une sauvegarde système (serveurs et applications de production) une fois par mois.

• Le support de sauvegarde journalière du lundi au jeudi est doublé et utilisé par alternance toutes les deux semaines.

8.3.2 Délai de conservation des sauvegardes

• Le support du vendredi est conservé 1 mois comme sauvegarde hebdomadaire.

• Le support du dernier vendredi du mois est conservé 1 an comme sauvegarde mensuelle.

• Le support du dernier vendredi de l'année est conservé sans limitation de durée comme sauvegarde annuelle.

8.4 Choisir le support de sauvegarde

8.4.1 Sauvegarde en interne

- Sur des supports de petit volume de stockage (DVD, clé USB, disque dur externe) Pour les opérations quotidiennes, utiliser le disque dur externe est simple, rapide et fiable.

Ce type de sauvegarde est préconisé pour des quantités d´information assez faibles. Le principe consiste à sélectionner les fichiers à sauvegarder poste par poste puis de procéder à leur sauvegarde.

Sur des bandes magnétiques ou cartouches numériques, Ces supports sont utilisés pour la sauvegarde de données stockées sur un serveur. Ils s'utilisent avec une application dédiée qui programme, gère et teste les enregistrements.

- Sur le serveur du réseau interne de l'entreprise Il s'agit de réserver un espace dédié à la sauvegarde sur le disque dur du serveur. Toutefois, préférez les modèles proposant une version amovible de ce disque dur de secours afin d'éviter qu'en cas de sinistre, le serveur et sa sauvegarde ne soient détruits.

Par ailleurs, il est possible de configurer le serveur pour que l'espace dédié à la sauvegarde soit une copie exacte en temps réel du disque dur principal.

Figure 54 : Moyen de sauvegarde

8.4.2 Sauvegarde à distance :

Elle consiste à sous-traiter la sauvegarde des données à un prestataire spécialisé dans l'hébergement. Cette solution offre l'avantage de ne plus avoir à gérer le support physique des sauvegardes ou la charge de travail associée, car ils sont externalisés via un réseau haut débit.

Toutefois, des risques associés à de mauvaises sauvegardes subsistent. Il est d'ailleurs nécessaire de bien définir les données à sauvegarder, leur dimensionnement et s'assurer que les sauvegardes sont bien réalisées.

8.5 Tester l'intégrité des données :

Fin de s'assurer du bon fonctionnement des sauvegardes, des tests réguliers d'intégrité et de restauration des données doivent être réalisés pour détecter d'éventuelles anomalies (erreur d'application ou support saturé).

Le test de restauration consiste à simuler un sinistre et à utiliser des sauvegardes pour que l'entreprise puisse reprendre son activité.

8.6 Le plan de sauvegarde :

Le plan de sauvegarde permet d'organiser la restauration des données en cas de sinistre. Ce document formel est utilisé au cas où plus rien ne fonctionne.

Il doit ainsi garantir la continuité de la disponibilité des données et des activités de l'entreprise. Il consiste principalement à prioriser les ressources informationnelles à restaurer (messagerie, documents internes…).

Le plan de sauvegarde doit être approuvé par la direction et testé périodiquement (au moins une fois par an) afin de s'assurer de son bon fonctionnement.

Conclusion du chapitre 3

Les systèmes d'information modernes sont exposés à des menaces contre lesquelles ils doivent impérativement être protégés. Pour ce faire, les méthodes d'analyses de risques permettent dans un premier temps de révéler les vulnérabilités de ces systèmes. Après quoi, il existe un certain nombre de solutions techniques qui permettent de mettre en œuvre des parades efficaces.

Le domaine de la cybersécurité est actuellement en pleine expansion, d'une part parce que les technologies évoluent et que les parades doivent s'adapter, et d'autre part parce que les attaquants développent sans cesse des nouvelles techniques pour essayer de contourner ces parades.

Conclusion générale

En conclusion, les systèmes d'information de l'entreprise jouent un rôle essentiel dans le fonctionnement, la compétitivité et la réussite globale des organisations modernes. Ils servent de colonne vertébrale pour la collecte, le stockage, la gestion et l'analyse des données, permettant aux entreprises de prendre des décisions éclairées, d'optimiser leurs processus opérationnels, de mieux comprendre leurs clients et leur marché, et d'innover dans un environnement en constante évolution.

Ces systèmes contribuent également à la communication interne, à la collaboration entre les départements et les équipes, et à la création d'une culture de l'information au sein de l'entreprise. De plus, ils renforcent la sécurité des données, garantissant que les informations sensibles sont protégées contre les menaces internes et externes.

Cependant, il est crucial de reconnaître que les systèmes d'information ne sont pas une solution miracle, mais plutôt un outil puissant qui doit être bien géré et adapté aux besoins spécifiques de chaque entreprise. Les défis liés à la cybersécurité, à la gestion des données, à l'intégration de nouvelles technologies et à l'adaptation aux évolutions du marché continueront de se poser.

En fin de compte, une stratégie de systèmes d'information bien planifiée et une gouvernance efficace sont essentielles pour maximiser les avantages potentiels tout en minimisant les risques. Les entreprises qui investissent judicieusement dans leurs systèmes d'information peuvent renforcer leur agilité, leur compétitivité et leur capacité à prospérer dans un monde des affaires de plus en plus numérique.

Bibliographie :

- **"Management Information Systems: Managing the Digital Firm"** par Kenneth C. Laudon et Jane P. Laudon - Cet ouvrage est une ressource incontournable pour comprendre les fondements des systèmes d'information du point de vue de la gestion et de l'entreprise.

- "Information Systems: A Manager's Guide to Harnessing Technology" par John Gallaugher - Ce livre offre une perspective axée sur la gestion des systèmes d'information et leur rôle dans la prise de décision stratégique.

- **"Information Systems Today: Managing in the Digital World"** par Joseph Valacich et Christoph Schneider - Il s'agit d'un manuel de référence qui explore les concepts clés des systèmes d'information, notamment leur impact sur les organisations.

- **"Enterprise Architecture As Strategy: Creating a Foundation for Business Execution"** par Peter Weill et Jeanne W. Ross - Ce livre se concentre sur la manière dont les systèmes d'information peuvent être alignés sur la stratégie de l'entreprise grâce à l'architecture d'entreprise.

- **"Introduction to Information Systems"** par R. Kelly Rainer Jr., Brad Prince, and Casey G. Cegielski - Cette introduction complète aux systèmes d'information couvre les principaux concepts et leur application dans le monde réel.

- **"Information Systems for Managers: Texts and Cases"** par Gabriele Piccoli et Federico Pigni - Ce livre offre une perspective internationale sur les systèmes d'information, en mettant l'accent sur les défis liés à la gestion.

- **"Information Technology for Management: On-Demand Strategies for Performance, Growth, and Sustainability"** par Efraim Turban, Linda Volonino, et Gregory R. Wood - Ce livre explore comment les technologies de l'information peuvent être utilisées pour améliorer les performances organisationnelles.

- **"Modern Database Management"** par Jeffrey A. Hoffer, Ramesh Venkataraman, et Heikki Topi - Un ouvrage qui se penche sur les bases de données, un élément crucial des systèmes d'information.

- **"Computer Networking: Principles, Protocols and Practice"** par Olivier Bonaventure - Ce livre explore les concepts fondamentaux des réseaux informatiques, allant des principes de base aux protocoles avancés.

- **"Computer Networks"** par Andrew S. Tanenbaum et David J. Wetherall - Une référence classique qui couvre de manière approfondie les concepts de réseaux, de la couche physique aux applications.

- **"Data Communications and Networking"** par Behrouz A. Forouzan - Un manuel complet qui explique les principes de la communication de données et des réseaux.

- **"Introduction to the Theory of Computation"** par Michael Sipser - Ce livre explore la théorie de la computation, un concept essentiel pour comprendre les systèmes d'information et les réseaux.

Généralités sur la Sécurité des Systèmes d'Information et des Réseaux :

- **"Network Security Essentials: Applications and Standards"** par William Stallings - Ce livre offre une introduction complète aux principes de base de la sécurité des réseaux.

- **"Computer Security: Principles and Practice"** par William Stallings et Lawrie Brown - Un ouvrage qui explore les concepts de sécurité informatique, de la cryptographie à la gestion des risques.

- **"CISSP All-in-One Exam Guide"** par Shon Harris - Un guide complet pour la certification CISSP (Certified Information Systems Security Professional) qui couvre l'ensemble des domaines de la sécurité informatique.

- **"Information Security Management Principles"** par David Alexander, M. David Sutton, et Andy Whitmore - Ce livre aborde les principes de gestion de la sécurité des informations, notamment la norme ISO 27001.

Cybersécurité et Menaces Informatiques :

- **"Hacking: The Art of Exploitation"** par Jon Erickson - Un ouvrage qui explore les aspects techniques du piratage informatique, avec une perspective axée sur la défense.

- **"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws"** par Dafydd Stuttard et Marcus Pinto - Un guide essentiel pour comprendre les vulnérabilités des applications web et comment les sécuriser.

- **"The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations"** par Ben Buchanan - Ce livre examine les défis de la cybersécurité à l'échelle nationale et internationale.

Sécurité des Applications Web et des Logiciels :

- **"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws"** par Dafydd Stuttard et Marcus Pinto - Un guide essentiel pour comprendre les vulnérabilités des applications web et comment les sécuriser.

- **"Secure Coding in C and C++"** par Robert C. Seacord - Un livre qui se concentre sur la sécurisation du code informatique dans les langages C et C++.

Sites web :

https://www.isc2.org/

https://www.sans.org/

https://csrc.nist.gov/

http://www.securityfocus.com/

https://www.cisecurity.org/

https://www.darkreading.com/

https://krebsonsecurity.com/

https://www.certmag.com/