# TABLE DES MATIERES

Page

# INTRODUCTION

Ce travail entre dans le cadre du cours de tronc commun du DEA-SI et MATIS. Ce cours touche le domaine des Systèmes d'Information et organisation.

A travers une brève description des services d'Internet démontrer et réfléchir sur les méthodes de mise en œuvre d'Internet et d'Intranet et de leur Sécurité. La description de (s) la méthodes nous permettra de mettre en exergue l'efficience en matière de mise en place et nous permettra aussi de nous poser les bonnes questions afin de donner quelque indications au entreprise pour réponde aux questions « On ne sais pas comment faire ?, On ne sais pas quoi faire ?….. ».

Vu la vaste liste des services d'Internet et d'Intranet, au cours de ce travail on se limitera à l'étude de l'implantation d'Internet, d'Intranet et des sites web car se sont les applications majeures de la toile au niveau publique et au niveau privé, sans oublier naturellement la Sécurité. L'analyse des méthodes de mise en place de ses services de bien définir les problèmes et les processus existants vis-à-vis de l'entreprise et de ses besoins.

Donc, pour arriver à ce résultat, nous commencerons, par donner quelques généralités sur Internet et Intranet pour passer dans un deuxième temps à l'étude des méthodes de mise en place et d'en dégager les difficultés. Et passer dans un troisième temps aux problèmes de Sécurité et des méthodologies qui sont liées à Internet et Intranet ainsi que les solutions pour les résoudre.

# I) Que signifie " Internet " ? :

## I. 1) Généralités sur Internet :

### I.1. a) Définition d'Internet :

Selon Richard J. SMITH, Le terme Internet est difficile à cerner, car il fait référence à d'innombrables services et possibilités ouvrant autant d'horizons jusque là inconnus. Pour certaines personnes, il n'est rien de plus qu'un moyen convenable et pratique d'envoyer du courrier électronique à d'autres utilisateurs. Pour d'autres, c'est un lieu de rencontre où l'on se fait des amis, où l'on joue, polémique, travaille et voyage à travers le monde.

Et Jean-Luc ARCHIMBAUD affirme dans son article que ….qui dit Internet dit réseau des réseaux. En effet c'est un immense réseau par le nombres d'utilisateurs et de stations, mais aussi par le nombres de liaisons et leurs débit. Ces stations (ou ordinateur) doivent parler le même langage dit en commun protocole notamment le protocole TCP/IP (Transport Control Protocol/Internet Protocol) pour pouvoir communiquer…. .

### I.1. b) Les Avantages et les Défauts d'Internet :

| Les Avantages | Les Défauts |
|---|---|
| • Il y a une égalité des ordinateurs et des individus.<br>• Il y a aussi l'abolition des distances et des frontières.<br>• La liberté totale d'expression est pratique courante.<br>• Les informations proviennent directement des sources (les propriétaires).<br>• L'esprit de gratuité des services.<br>• Les utilisateurs acceptent de partager leur expérience. | • C'est un vrai labyrinthe.<br>• Il est important d'avoir un initiateur.<br>• Il y a tout et n'importe quoi comme informations, donc, aucune possibilité de vérifier.<br>• Facilité de propagation des virus.<br>• Quelques problèmes de sécurité des réseaux.<br>• Le service n'est pas toujours garanti (ex : changement de localisation d'une information) |

### I.1. c) Que nous offre Internet ? :

On peut regarder l'Internet avec les lunettes d'un économiste comme un ensemble de consommateurs et de producteurs d'information. Un consommateur utilise Internet pour travailler avec une informatique distribuée (connexion en mode terminal sur un ordinateur distant, transfert de fichiers entre ordinateurs, exécution partagée de programmes entre plusieurs stations...) ou accède à des informations de tous types (textes, images fixes ou animées, sons, sous différents formats) dans des bases de données distribuées avec des outils logiciels très divers (FTP anonymous, WAIS, Gopher, Archie, WWW...).

Ces ressources et ces informations proviennent de producteurs. Ceux-ci peuvent mettre à disposition, rendre accessibles, en contrôlant les accès et éventuellement en facturant,

leurs équipements informatiques (serveurs de calcul, disques, imprimantes...) ou leurs différentes informations (bases de données). De nombreux sites sont à la fois consommateurs et producteurs, ainsi cette distinction n'est pas exclusive.

Les services de l'Internet sont en fait toutes les applications que l'on peut utiliser avec les protocoles de communication TCP/IP. Elles sont très nombreuses et de nouvelles apparaissent régulièrement. Elles fonctionnent en mode Client/Serveur et il y a donc pour chaque service un logiciel client et un logiciel serveur. Pour une application, le dialogue entre le logiciel client et le logiciel serveur, le protocole, est généralement décrit dans une **RFC (*Request For Comment*)** qui est le standard à respecter.

Par commodité, on peut classer les services en trois familles : **Classiques** (ou de Type Informatique : Telnet et FTP), d'**Accès à l'information** (ou Outils de Diffusions : FTP anonymous, Wais, Gopher, WWW, …) et de **Communication entre personnes** (ou Outils de Dialogues : E-Mail, News, Newsgoup , vidéoconférence, travail en groupe, …).

## I.1. d) Les Coûts d'Internet :

Selon "<<C'est gratuit !>> dit le chercheur. <<C'est hors de prix !>> dit le P-DG de la PME.". Malgré, les impressions de nombreux utilisateurs, Internet n'est pas gratuit. Il y a d'abord les coûts d'utilisation des serveurs distants ou de consultation de Bases de données. Ces coûts sont exprimés sous forme de "**Forfait**" ou abonnement mensuel ou annuel mais le prix dépend du débit de la liaison.

Et dans le cas d'un accès par réseau téléphonique, il faudra y ajouter un coût horaire de connexion téléphonique. De leur côté, les réseaux des prestataires de services sont financés par leurs clients, avec différents types de facturation, le forfait étant le principal modèle. Un schéma similaire se retrouve souvent dans les autres pays. Tout ceci nous permet d'en déduire que c'est les utilisateurs (clients, prestataire local ou régional ou…, opérateurs, Provider, …) qui financent les services fournis sur le réseau et chacun à un certain niveau.

# I. 2) Les Services et Applications d'Internet :

## I.2. a) La Messagerie (E-Mail) :

Maintenant très répandu, elle permet de s'affranchir des interruptions téléphoniques et des décalages horaires. Chaque utilisateur possède une adresse unique (adresse électronique ou Email), souvent de la forme **Prenom.Nom@nom_de_domaine.fr**, comme allal.mennis@esa.upmf-grenoble.fr.

La messagerie se base sur les principes de la communication suivants : communication en temps différé entre expéditeur et destinataire, pas de connexion directe entre les terminaux expéditeur et destinataire et mise en mémoire du message / analogie de la boite aux lettres (BAL).

**Les avantages :** Disponibilité, Efficacité, Mobilité, Simplicité d'utilisation et flexibilité, Rapidité, Données exploitables, Communication de groupe et Maîtrise des communications (la communication n'est pas plus imposée).

**Les protocoles de messagerie :** Le protocole standard utilisé sur l'Internet, est **SMTP** ainsi que **MIME**, **POP** et **IMAP**.

## I.2. b) Le service FTP :

FTP (File Transfert Protocol) est un outil indispensable pour transférer des données entre ordinateurs sur Internet. C'est aussi un protocole standard de haut niveau pour transférer des fichiers d'un nœud (unité d'interface ou solution sur réseau) à l'autre, il fonctionne quel que soit le type d'ordinateur utiliser et quelle que soit la machine de l'autre côté de la connexion. Un des atouts remarquables des logiciels FTP, c'est la vitesse avec laquelle les fichiers peuvent être envoyer et/ou reçus à travers Internet. Certains logiciels sont disponibles gratuitement. Cette gratuité se décline sous deux aspects :

**Les Freeware :** Les logiciels dits Freeware sont des logiciels gratuits dont certains son même disponible en code source, leurs auteurs les offrent gratuitement à la communauté navigante, car ce sont des êtres altruistes et généreux.

**Les Shareware :** Les logiciels Shareware sont des programmes que leurs auteurs souhaitent que nous échangions entre nous utilisateurs, chose qui n'est innocente. En effet, dans le premier cas de figure, il va falloir payer la licence d'exploitation du produit, et dans le deuxième cas, le logiciel aura une durée d'utilisation et de vie limitée (ou version d'évaluation) à 30 jours en moyenne, ce qui nécessite une réinstallation à terme sinon on sera dans l'obligation d'acheter la version définitive.

**Le FTP anonyme :**

Les utilisateurs appellent ce serveur avec un logiciel client FTP, entrent "anonymous" comme nom d'utilisateur et leur adresse électronique comme mot de passe. Puis ils utilisent les commandes classiques de FTP. Il est souvent utilisé pour télécharger sur l'ordinateur des fichiers provenant d'autres ordinateurs autorisant un accès public aux fichiers. Grâce à la connexion FTP anonyme, on a pas besoin de mot de passe ou de compte pour accéder à un ordinateur hôte éloigné. Seuls les fichiers du répertoire réservé au publics sont disponibles.

## I.2. c) Le service Telnet :

Telnet est un programme mettant en œuvre le protocole TELNET, basé sur la suite des protocoles TCP/IP en utilisant une architecture Client/Serveur. Les deux acteurs du scénario Client/Serveur négocient entre eux pour savoir comment ils vont procéder à la connexion et se mettre d'accord sur une langue commune. Le service Telnet permet d'utiliser un micro ou une station de travail comme un terminal raccordé à un ordinateur. Sauf exception, pour accéder à cet ordinateur il faut y avoir un compte, un nom et un mot de passe.

Toute fois, Telnet n'est pas sans limites. Si le trafic de données devient trop important sur l'un des réseaux qui vous relient à l'ordinateur éloigné, les échanges pouvons être très lents, nuisant à la procédure.

## I.2. d) Le Site Web de l'entreprise :

**Généralités :**

- Le web est un média à part entière.

- Définir l'objectif du site à réaliser.
- Insérer ce service dans une politique de communication globale.
- Promouvoir le serveur et le faire vivre.

**Les différents styles de sites :** le site "Plaquette", le site "Communication Institutionnelle", les sites "Transactionnels" et dans les cas d'appel à des prestataire extérieurs.

**Les compétences nécessaires :** Technicien, Graphiste, Maquettiste, Rédacteurs et Chef de projet.

**Les conseils à retenir :** Faire attention à l'ergonomie, Eviter les images trop lourdes, Formulaire de retour, Prévoir le bon personnel pour maintenir le serveur, Exiger des statistiques de consultation, Mettre très souvent le serveur à jour et Promouvoir le service en ajoutant des liens vers d'autres sites.

## I.2. e) Le Commerce Electronique :

Selon le rapport du groupe de travail présidé par M. Francis LORENTZ sur le commerce électronique pour le compte du Ministère des Finances Français : « Le Commerce Electronique couvre, à la fois, les échanges d'information et les transactions concernant des produits, équipements ou biens de consommation courante et des services (services d'information, financiers, juridiques...). Les moyens ou modes de transmission utilisés peuvent être divers : téléphone, télévision, Minitel, réseaux informatiques, Internet, etc. Leur caractéristique commune est de traiter de l'information numérisée incluant données, texte, son et images. »

Et selon la commission "Commerce Electronique" du Chapitre Français de l'Isoc, elle considère que le commerce électronique est avant tout du commerce et que le réseau n'est qu'un moyen ou support de communication. Et elle recommande de bien distinguer le commerce entre entreprises (Business to Business, B2B) et le commerce avec les particuliers (Business to Consumer, B2C). Il est évident que ces deux domaines partagent des technologies et des techniques et le "**médium**" Internet, mais leurs contextes réglementaires et contractuels respectifs, qui sont fort différents, nous paraissent plus importants que les outils communs.

## I.2. f) Le service Archie :

Archie est une sorte de bibliothécaire géant qui explore régulièrement et automatiquement de nombreux serveurs d'Internet et indexe leurs fichiers pour créer une base de données. Cette base de données constitue par conséquent un index de répertoires, une compilation de tous les fichiers disponibles de chaque serveur interrogé par le programme Archie. Donc, Archie n'est pas un seul système, mais, une collection de serveurs. Archie est basé sur une architecture Client/Serveur.

Toute fois, Archie n'est pas sans limites. Ses bases de données contiennent uniquement les fichiers des serveurs accessibles via FTP. Par conséquent, les sites accessibles uniquement aux utilisateurs disposant d'un nom et login ne sont pas inclus dans les bases de données d'Archie. Une autre limite du programme, est qu'il ne sait rien sur le fichier chercher. Il ne propose aucune information sur le contenu du fichier et ne dit pas s'il s'agit d'un programme ou d'un fichier texte ou d'une base de données.

## I.2. g) Le service WAIS :

WAIS a été un des 1er programmes à être bâti autour de la norme internationale Z39.50 similaire au langage SQL, qui est une définition de services de récupération d'informations et spécifications pour normes de programmes de bibliothèque. Tous les serveurs WAIS sont accessibles à tous les clients et sont censés être capables de se connecter à toutes les bases de données étant donner que la plupart des bases de données sur Internet utilisent des procédés différents pour stocker les données et pour y accéder.

Le client pose une question avec une suite de mots clés à un ou plusieurs serveurs qui hébergent de telles bases. Il reçoit en retour une liste de descripteurs de documents. Il peut ensuite transférer ces documents sur sa station, s'il le désire. Il existe un annuaire mondial des bases WAIS "directory-of-servers" gérée par la machine quake.think.com et un annuaire des bases françaises, "directory-zenon-inria-fr" sur la machine zenon.inria.fr.

Les limites de WAIS viennent du fait qu'on ne peut pas effectuer des recherches de texte français (les base de données à votre disposition sont en langue anglaise), les caractères génériques ne sont pas disponibles. La logique booléenne non plus n'est pas applicable dans la plupart des recherches via WAIS. Autrement dit, on ne peut rien faire d'autre que de chercher un mot ou plusieurs mots.

## I.2. h) La Visioconférence :

Comme son nom l'indique, la visioconférence permet à deux interlocuteurs, voire d'avantage, de communiquer verbalement en se voyant. Le but de la visioconférence est de réussir, voir, décider en direct et indépendamment, d'investissement accessible et de réduction des frais de fonctionnement.

La visioconférence offre plusieurs gains à l'entreprise notamment, une réaction rapide aux évolutions du marché, permet la gestion du développement de l'entreprise, une dynamisation de la communication interne, amélioration de la gestion des ressources humaines et une meilleure disponibilité des cadres.

## I.2. i) Le service Gopher :

Gopher est un système Client/Serveur pouvant être utilisé sur un grand nombre de machines, dont UNIX, DOS, WINDOWS et X-windows. Il ne s'agit pas d'un seul index, mais de nombreux index distribués depuis des centaines d'emplacements différents et reliés entre eux par des milliers de liaisons. Le logiciel client tourne sur notre ordinateur peut négocier avec tous les serveurs Gopher. Si le système informatique local comprend un serveur Gopher, c'est probablement là qu'on commencera l'apprentissage. Dans le cas contraire, notre client Gopher pourra accéder à n'importe quel serveur Gopher sur Internet.

Il présente à l'utilisateur les documents disponibles sur l'Internet comme un immense arbre similaire à un système de fichiers, où chaque fichier peut être sur n'importe quel serveur de l'Internet. L'utilisateur peut se promener dans l'arborescence, visualiser un document sur son écran, rapatrier un fichier sur son poste de travail pour le stocker localement et interroger des bases de données indexées en fournissant des mots clé. Ce service est maintenant de plus en plus remplacé par www, mais la base existante perdure.

# II) Qu'est ce que " Intranet " ? :

## II. 1) Le concept Intranet :

On peut définir le concept Intranet comme étant l'utilisation de tout ou partie des technologies et des informations d'Internet pour les besoins de transport et de traitement des flux d'informations internes d'un groupe d'utilisateurs identifiés. Ce concept est lié aussi à la maîtrise d'un réseau en garantissant la qualité des services, ses évolutions et la sécurité. Il ne faut pas oublier que c'est un Internet privé. Les protocoles utilisés dans les Intranets sont : TCP/IP, SNMP, FTP et NFS, X-windows, SMTP, POP et IMAP, NNTP, LDAP/X500 et HTTP, CGI et HTML.

## II. 2) Les services et les fonctionnalités Intranet :

Un Intranet nous offre des services dont les outils de communication interne, la base de connaissance de l'entreprise, la messagerie, l'agenda partagé, le Groupware, des forums de discussion et les services classiques de réseau local. Pour comprendre et cerner l'importance actuelle d'Intranet regardons de plus près tous les services et fonctionnalités :

### II.2. a) Les services de partage d'information :

**Les serveurs de fichiers :** sur un Intranet, les serveurs de fichiers sont souvent les serveurs de fichiers classiques des systèmes d'exploitation utilisés. Notamment avec l'utilisation de NFS. Il y a aussi le transfert de fichiers qui s'appuie le plus souvent sur le protocole FTP.

**Les serveurs de documents :** les serveurs de documents dans un Intranet permettent aux utilisateurs de rechercher et de consulter l'ensemble des produits par l'organisation. Les serveurs sont dans la plupart des cas des serveurs Web vu qu'ils facilitent l'implantation des moteurs de recherches et surtout en texte intégral.

**Les serveurs de données (Base de Données) :** les Bases de Donnés sont celles fondés sur les standards du marché, notamment SQL. Elles s'interfacent avec elles aussi avec les services Web pour être consultées.

**Les services de production et de publication d'information :** pour que l'information soit consultable par tous sur un Intranet, il faut que les outils et les suites bureautiques utilisent le même format à la sortie. Le format le plus utilisé dans ce cas est le format HTML qui est le standard de présentation de l'information sur Intranet et aussi sur Internet.

### II.2. b) Les services de communication et de travail coopératif :

**La messagerie et les listes de diffusion :** la messagerie d'un Intranet ressemble trait pour trait aux messageries propriétaires que nos SI ont vu fleurir ces dernières années. L'utilisation des listes de diffusion dans les Intranets des entreprises intervient au niveau des projets de nouveaux produits, pour les comités d'entreprise, pour les annonces, les résultats commerciaux, …

**La circulation de documents :** la circulation de documents est une extension naturelle de la messagerie et dans tous les cas, il s'agit de coller au mieux au processus de l'entreprise.

**La visioconférence et l'audioconférence :** les outils de la visioconférence trouvent toute leur puissance sur un Intranet.

**Les forums :** les services de forums suivent de très près la messageries et/ou les serveurs Web dans la construction d'un Intranet. Il y a 2 types de forums qui sont utilisées : les forums interactifs en temps réel et les forums interactifs en temps différé.

### II.2. c) Les services d'annuaires :

Les annuaires permettent de retrouver les adresses et les droits de chacun des utilisateurs de l'Intranet. Les mécanismes les plus utiliser sont X500 et LADP. Il y a aussi l'annuaire des catalogues et des indexe des informations produites. Il faut y rajouter l'annuaire des clés de chiffrement.

## II. 3) Les avantages et les défauts d'Intranet :

| Avantages | Défauts |
|---|---|
| • Fin des incompatibilités.<br>• Plus d'indépendance par rapport aux fournisseurs informatique.<br>• Améliorer la circulation interne de l'information.<br>• Gagner du temps.<br>• Simplifier l'utilisation des outils informatiques.<br>• Rapprocher les services.<br>• Permet de construire progressivement un SI souple et évolutif.<br>• Pérenniser le SI par la standardisation.<br>• Simplifier l'administration du SI.<br>• Faciliter le partage de l'information.<br>• Communication interentreprises.<br>• Confidentialité et sécurité.<br>• Economies sur les coûts de communication.<br>• Economies sur les télécommunications. | • Intranet ne couvre pas tous les besoin du SI.<br>• Complexité technologique.<br>• Lenteur.<br>• Problèmes de confidentialité de l'information.<br>• Manque de compétences techniques.<br>• Trop d'informations.<br>• Coûts élevés.<br>• Nécessité de personnel pour alimenter le site.<br>• Jeunesse de certaines technologies. |

# III) La mise en œuvre d'Internet et d'Intranet ?

## III. 1) La mise en œuvre d'Internet :

Pour la mise en œuvre, l'entreprise doit suivre une méthodologie rigoureuse. Un projet bien pensé dès le départ pourra éviter bien des désagréments par la suite. Le projet de mise en place passe par le respect de la formule suivante :

**Connexion Internet**
**=**
**Réflexion + Information + Installation + Formation**

Ces phases sont nécessaires et obligatoires pour la réussite du projet.

### III.1. a) Définir les besoins et les objectifs :

Avant de se connecter physiquement, l'entreprise devra comme pour tout projet informatique, passer par une phase de réflexion sur l'utilisation qu'elle désire faire d'Internet. Les questions suivantes devront trouver des réponses claires et précises :

- Quels sont mes besoins en termes de communication interne ?.
- Quels sont mes besoins en termes de communication avec mes fournisseurs, mes clients et mes prospects ?.
- Est-ce que je désire être utilisateur du réseaux (rechercher des informations) ou mettre à la disposition des usagers de l'Internet des informations ma société ?.
- Dois-je rechercher une communication de personne à personne (de type messagerie) ou basée sur le document (services W3 ou Gopher) ?.
- Si je désire mettre en place un service W3, quelle information dois-je présenter et comment la traiter (mise en place de bons de commandes, informations en ligne, type de télépaiement, quelle démarche de sécurité) ?.
- Dois-je créer le service ou me faire héberger ?.

### III.1. b) Informer le personnel :

Le projet Internet devra également être bien compris, assimilé et accepté par ses utilisateurs au sein de l'entreprise. Sans information au départ, les utilisateurs risquent de mal assimiler le phénomène culturel représenté Par Internet.

Cette Information peut se faire sous forme de réunions, rassemblant certains profils communs : une demi-journée avec les personnes à caractère plus commercial, une avec celles dont le travail est plutôt de type administratif, puis technique, etc.

Bien entendu, le discours sera adapté au profil de chacun des groupes de personnes. Une démonstration simple des possibilités d'Internet sera également une bonne chose pour mieux visualiser la portée des outils disponibles.

## III.1. c) Comment réussir la connexion ? :

Il existe une multitude de possibilité pour connecter l'entreprise à Internet. Nous nous pencherons donc plus spécifiquement sur les deux solutions de connexion aujourd'hui les plus utilisées par les entreprises.

### c1) La connexion directe :

Elle se fait par l'intermédiaire d'une liaison louée entre le site informatique et celui de l'opérateur Internet. Votre réseau est connecté à celui de l'opération Internet (au moyen de routeurs) par l'intermédiaire d'une liaison Transfix ou Transpac. Les boîtes aux lettres E-mail des utilisateurs de votre entreprise sont gérées par un logiciel spécifique sur votre site. Vous êtes connecté au réseau 24 heures sur 24.

Seuls les opérateurs Internet donnent aujourd'hui l'accès à ce type de connexion. La facturation auprès de cet opérateur peut être de deux types : forfaitaire ou au prorata du volume d'informations échangées.

Les postes de coût, comme le verrons plus loin, sont alors les suivants :

*Coûts d'investissement :*

- Installation initiale de la liaison louée.
- Achat d'un routeur (sont coût est parfois compris dans les frais d'installation d la liaison louée).
- Coût initial de la mise en place de l'accès chez l'opérateur Internet (parfois).

*Coûts de fonctionnement :*

- Abonnement mensuel à la liaison louée.
- Abonnement auprès de l'opérateur Internet.

### c2) La connexion Dial-up IP :

La connexion Dial-up IP est assez comparable à la connexion directe, puisque vous aurez, si votre besoin est uniquement de rechercher de l'information, pratiquement les mêmes logiciels sur vos ordinateurs. Mais la connexion ne se fera plus par le biais d'une liaison louée, mais par le réseau téléphonique (RTC) ou une liaison Numéris (RNIS) :

On ne parle plus ici de retours, seuls un ou des modems (adaptateurs Numéris) suffiront à la connexion. La connexion en Dial-up IP est proposée par les opérateurs Internet et les offreurs de connexion. L'abonnement peut-être soit au forfait, soit à la durée, soit au volume d'informations échangées. Dans ce cas, le mieux est une facturation au forfait, elle

vous permettra de gérer plus efficacement vos budgets.

Pour l'E-Mail, l'offreur de connexion hébergera vos boîtes à lettres sur son site. Vous vous connectez à la demande, soit pour rapatrier sur votre machine les messages qui vous ont été envoyés, soit pour envoyer vos propres messages.

Les postes de coût seront alors les suivants :

*Coûts d'investissement :*

- Coût du ou des micro-ordinateur(s) et modem(s), si vous ne les avez pas déjà. Dans le cas d'une liaison Numéris, le coût de l'adaptateur (à la place du modem) est compris dans les frais d'installation de la ligne.
- Coût initiale de mise en place de l'accès chez l'opérateur Internet (parfois).
- Coût initial de la mise en place de la liaison RNIS ou éventuellement d'une ou plusieurs lignes téléphoniques.

*Coûts de fonctionnement :*

- Coût des communications téléphoniques (cas du RTC) ou Numéris.
- Abonnement auprès de l'opérateur Internet.

## III.1. d) Combien coûte une connexion ? :

Il est très difficile de donner des coûts exhaustifs, nous allons essayer de donner des fourchettes de prix selon l'utilisation que vous désirez faire du réseau.

### d1) La connexion d'un poste isolé pour l'E-Mail :

Vous désirez connecter une seul machine de votre entreprise sur Internet. Une connexion directe n'est pas à envisager car elle coûterait trop cher. La seul solution viable est le Dial-up IP en RTC. La connexion Numéris n'apporterait pas gros avantages car les temps de transmission d'information sont relativement courts avec un outil comme la messagerie.

| **Connexion d'un poste isolé pour l'E-Mail** | |
|---|---|
| **Coûts d'investissement** | |
| Micro-ordinateur | 5 000 à 15 000 Frs |
| Modem | 1 000 à 2 000 Frs |
| Logiciels | 0 à 2 000 Frs |
| Coût initial de raccordement chez le fournisseur | 0 à 1 000 Frs |
| Installation d'une ligne téléphonique | 45 Frs |
| **Coûts de fonctionnement** | |
| Coûts fournisseur | 100 à 800 Frs/mois |
| Coûts téléphoniques | 25 Frs/mois |

Les coûts en logiciels peuvent être nuls (si le choix se porte sur l'option de n'utiliser que des logiciels en Freeware) ou de l'ordre de 500 à 1000 Frs (si vous achetez un produit "packagé" dans le commerce).

## d2) La connexion d'un poste isolé pour l'E-Mail et la consultation de services :

L'utilisation d'Internet ne se limitera pas ici à la messagerie électronique. Tous les outils fournis par le réseau pourront être utilisés (FTP, News, navigation sur les services Gopher ou Web, …), ce qui induira un temps de connexion moyen bien plus long.

### Le cas d'une connexion RTC :

| Connexion d'un poste isolé pour l'E-Mail et la consultation de services en RTC | |
|---|---|
| **Coûts d'investissement** | |
| Micro-ordinateur | 5 000 à 15 000 Frs |
| Modem | 1 000 à 2 000 Frs |
| Logiciels | 0 à 2 000 Frs |
| Coût initial de raccordement chez le fournisseur | 0 à 250 Frs (en moyenne) |
| Installation d'une ligne téléphonique | 45 Frs |
| **Coûts de fonctionnement** | |
| Coûts fournisseur | 100 à 1 000 Frs/mois |
| Coûts téléphoniques | 150 Frs/mois |

### Le cas d'une connexion Numéris :

| Connexion d'un poste isolé pour l'E-Mail et la consultation de services en Numéris | |
|---|---|
| **Coûts d'investissement** | |
| Micro-ordinateur | 5 000 à 15 000 Frs |
| Adaptateur | Compris dans le coût de mise en place |
| Logiciels | 0 à 1 000 Frs |
| Coût initial de raccordement chez le fournisseur | 380 à 500 Frs (en moyenne) |
| Installation d'une liaison Numéris | 800 Frs |
| **Coûts de fonctionnement** | |
| Coûts fournisseur | 2 000 à 2 5000 Frs/mois |
| Coûts Numéris | 380 Frs/mois |

Le tableau précédant montre bien que la solution Numéris n'est pas à privilégier dans ce cas figure, sauf si vous désirez à tout prix avoir accès à un débit assez fort. Il deviendra par contre plus intéressant dans un cas de fort trafic (par exemple, plusieurs dizaines d'heures de connexion par mois).

## d3) La connexion d'un réseau de machines pour l'E-Mail :

La solution envisagée ici sera la mise en réseau d'un certain nombre de modems, à l'aide d'un boîtier partageable, qui permettra à chaque utilisateur du réseau d'avoir un accès à Internet.

Supposons un réseau de 20 machines. Deux à trois modems seront suffisants dans ce cas. L'entreprise devra donc installer trois lignes téléphoniques (il est conseillé d'installer des lignes directes). On suppose que les micro-ordinateurs sont déjà présents sur le site. Ils ne sont donc pas comptabilisés dans les frais d'investissement. On estime que chaque machine générera un trafic de 5 minutes de connexion par jour, soit 100 minutes par mois, soit 2 00 minutes (33 heures) mensuelles pour le réseau total :

| Connexion d'un réseau de machines pour l'E-Mail | |
|---|---|
| **Coûts d'investissement** | |
| 3 Modems | 3 000 à 6 000 Frs |
| Logiciels | 0 à 3 000 Frs |
| Coût initial de raccordement chez le fournisseur | 0 à 2 500 Frs |
| Installation trois lignes téléphoniques | 135 Frs |
| **Coûts de fonctionnement** | |
| Coûts fournisseur | 2 600 à 3 600 Frs/mois |
| Coûts téléphoniques | 490 Frs/mois |

Il est très difficile de définir le coût de l'opérateur pour la connexion d'un réseau dans ce type de configuration. Il existe en effet deux types d'offres : dans le premier cas, le fournisseur considère votre réseau de façon global quel que soit le nombre de machines connectées, plus un coût à l'heure de connexion; dans le deuxième cas, le fournisseur vous demande un coût d'abonnement mensuel par machine plus un coût horaire.

## d4) La connexion d'un réseau de machines pour l'E-Mail et la consultation de services :

Une configuration technique identique à celles du cas précédant sera retenu dans ce cas de figure, la seul différence étant l'utilisation beaucoup plus intensive des outils d'Internet. Les chiffres retenus dans cet exemple sont : 10 heures mensuelles de connexion par machine, soit 20 heures pour l'ensemble du réseau.

| Connexion d'un réseau de machines pour l'E-Mail et la consultation de services | |
|---|---|
| **Coûts d'investissement** | |
| 3 Modems | 3 000 à 6 000 Frs |
| Logiciels | 0 à 3 000 Frs |
| Coût initial de raccordement chez le fournisseur | 0 à 2 500 Frs |
| Installation trois lignes téléphoniques | 135 Frs |
| **Coûts de fonctionnement** | |
| Coûts fournisseur | 10 000 à 20 000 Frs/mois |
| Coûts téléphoniques | 2 920 Frs/mois |

La solution Numéris pourrait sembler plus intéressante mais, tous calculs faits, on obtient à peu près les mêmes chiffres que ci-dessus pour une configuration identique.

## d5) La connexion par liaison louée d'un réseau de machines pour l'E-Mail et la consultation de services :

La configuration technique est identique au cas précédant et l'estimation en nombre d'heures de connexion, *via* un routeur, par liaison louée de type Transfix.

| Connexion d'un réseau de machines pour l'E-Mail et la consultation de services | |
|---|---|
| **Coûts d'investissement** | |
| Routeur | 20 000 Frs |
| Logiciels | 0 à 3 000 Frs |
| Coût initial de raccordement chez le fournisseur | 9 000 à 13 000 Frs |
| Installation d'une liaison Transfix à 64 Kbps | 4 750 Frs |
| **Coûts de fonctionnement** | |
| Coûts fournisseur | 5 000 à 6 000 Frs/mois |
| Coûts Transfix | 2 480 Frs/mois |

Les coûts fournisseur sont parfois plus élevés mais le chiffre indiqué ici semble être une bonne moyenne. La tarification n'est jamais appliquée au nombre d'heures, mais au forfait ou au volume d'informations échangées. On s'aperçoit très rapidement que dès que le trafic dépasse un certain nombre d'heures par mois, la mise en place d'une liaison louée devient rentable par rapport à la connexion Dial-up IP.

## III.1. e) La démarche de sécurité :

Il n'est certes pas question d'affirmer ici que l'utilisation des réseaux informatiques est sans danger. Les risques existent réellement et peuvent représenter de lourdes pertes en cas d'attaque. Il existe deux façons principales d'utiliser Internet : la communication de personne à personne et de personne à serveur.

Le plus gros risque induit par la communication d'informations par messagerie est l'interception de vos messages par une personne malveillante ou un mauvais aiguillage de ceux-ci les acheminement vers un destinataire non approprié. Si ce dernier type de problème arrive finalement assez peu souvent, personne n'est toute fois à l'abri d'un tel désagrément. En ce qui concerne la malveillance de pirates éventuels, on peut considérer que le nombre colossal d'information transitant à travers le réseau constitue déjà en soi une assez bonne protection. Pour remédier à ces inconvénients du côté de l'utilisateur, la solution serait de chiffrer soit le contenu des messages, soit certaines informations confidentielles.

En complément des technologies de cryptage, il existe également des systèmes d'authentification, d'horodatage et de certification des messages qui permettent d'être sûr que ceux-ci ont bien été envoyés et reçu ou d'apporter la preuve d'éventuelles falsification.

L'autre problème posé par la messageries est l'import de virus contenu dans un fichiers qui vous aurait été envoyé, attaché à une missive. La solution est simple : la très large gamme de logiciels anti-virus devrait minimiser très fortement tout risque de ce genre.

En fin les plus gros risques à l'heure actuelle se trouvent dans l'installation d'un serveur pour mettre à la disposition des usagers du réseau des informations sur l'établissement et ses produits, voire pour faire de la vente par correspondance. En effet en mettant en place ce type de projet, vous installez 24 heures sur 24 sur le réseau une fenêtre ouverte sur votre site informatique, laissant ainsi aux "hackers" libre cours à leur malveillance.

La première solution consiste à isolé physiquement le serveur de votre site informatique afin que toute intrusion ne soit pas équivalente à un pillage en règle de toutes les informations relatives à votre entreprise.

Une autre solution consiste à installer des logiciels de type Firewalls (appelés "Coupe-Feu" ou "Garde-Barrière") qui prémunissent le serveur d'éventuelles qui prémunissent le serveur d'éventuelles attaques de l'extérieur. Ces systèmes n'assurent pas protection ultime, mais retardent toute intrusion suspecte en avertissant l'administrateur du réseau qu'une manœuvre malveillante est en cours ou a été effectuée. Il convient d'ailleurs de dire ici qu'il n'existe aucun système de sécurité inhabile à 100%.

## III.1. f) Les raisons de choisir son Provider :

Le choix d'un fournisseur de connexion Internet ne se résume pas à l'unique aspect des coûts. L'offre de connexion doit être complète de nombreuses questions sont à poser aux entreprises que vous allez contacter :

- **Disponibilité des lignes d'accès dans le cas d'une liaison Dial-up**. Il faut essayer, le plus souvent possible, d'obtenir de l'entreprise son ratio client/modems. Plus ce ratio sera faible, meilleure sera la disponibilité des lignes. Plus ce ratio sera fort, plus sous aurez de chances de voir vos appels ne pas aboutir, tous les modems étant occupés. Reste à vérifier que le ratio avancé par l'entreprise est exact.

- **Conseils et fourniture de logiciels :** un fournisseur de connexion n'est pas a priori qu'un "vendeur de tuyaux". Il doit être capable de vous conseiller pour trouver la meilleure solution technique pour votre connexion. Il doit également pourvoir vous fournir les logiciels Freeware indispensable à vos premières connexions. Il doit vous offrir un service en même temps qu'il vous ouvre une porte sur Internet

- **Formation :** l'entreprise peut également vous fournir une prestation de formation de votre personnel à l'utilisation du réseau.

- **Maintenance :** ce n'est pas tout de vous connecter à Internet, il faut aussi que la solution choisie ne vous cause pas de soucis lors de son fonctionnement. L'infrastructure technique interne du fournisseur de connexion ainsi que ses aptitudes à assurer un suivi efficace (contrat de maintenance, possibilité de télémaintenance, délai d'intervention en cas de problème, …) seront des données extrêmement importantes dans votre choix.

- **Pérennité économique :** un grand nombre de sociétés dans le domaine d'Internet sont des *start-ups* dont il est difficile de mesurer aujourd'hui la pérennité. Le marché d'Internet étant encore jeune et n'ayant pas eu le temps de véritablement mûrir, il sera bien venu de prendre toutes les dispositions nécessaires pour vérifier que tel fournisseur a plus de chances qu'un autre d'être encore là dans un an.

Une des solutions les plus efficace pour avoir des renseignements fiables sur l'entreprise est de chercher puis de contacter quelques-uns de ses clients pour connaître leur expérience et leur vécu.

### III.1. g) Plan de formation :

Internet est une immensité dans laquelle on ne s'aventure pas à l'improviste. Les personnes qui seront connectées sur le réseau dans votre entreprise devront avoir été formées au préalable pour éviter de se perdre dans la jungle des services existants.

Cette phase de formation est capitale car il est très courant de voir des personnes rechercher des informations sur le réseau et naviguer des heures durant sans trouver le moindre renseignement et donc se décourage très vite, tout simplement par manque d'information et de formation préalable et cette aisance dans la navigation ne s'acquiert pas en un jour. Il va falloir prévoir un budget important pour ce poste car sinon, c'est l'ensemble de votre projet qui pourrait prendre l'eau.

## III. 2) La mise en œuvre d'Intranet :

Construire un Intranet est plus qu'un simple assemblage de briques techniques venant d'Internet. Un Intranet s'appuie en effet sur des concepts forts, qui le différencient des approches informatiques traditionnelles et qui posent les bases des SI des prochaines années.

### III.2. a) Les 4 principes fondamentaux de la mise en place d'un Intranet :

#### a1) Standardiser les composantes du SI :

L'approche qui s'appuie sur les produits d'un seul fournisseur, reflète un souci de cohésion et de performances. Les dangers de cette approche sont que l'évolution du SI est très liée au dynamisme et la capacité de réponse du fournisseur même si cette évolution est lente et difficile, il ne faut pas aussi négliger l'énorme désavantage du rapport coût/fonctionnalité.

On peut adopter une autre approche qui s'appuie sur les normes définies par de grands organismes mondiaux même si le décalage entre le temps de conception de la norme et le temps de sa mise sur le marché est trop long.

Pour garantir la pérennité, un Intranet s'appuie sur l'utilisation d'éléments ouverts et interchangeables. Ce mouvement a été amorcé par le Client/Serveur, il y a quelques années. Il s'agit de construire un SI modulaire, puissant, mais qui utilise des standards techniques du marché.

Si un autre fournisseur propose des produits aux fonctionnalités ou à des coûts plus intéressants, on remplacera la brique existante par ce nouvel élément. L'ensemble du système ne sera pas remis en cause.

Dans la construction d'un Intranet on fait donc le choix :

- de ne choisir que de technologie standardisées par le marché, utilisées par tous et vendues par de nombreux fournisseurs.

- de ne jamais s'enfermer dans des produits spécifiques dont on ne pourrait se sortir qu'avec peine et à grands frais.

### a2) Recentrer le SI sur le serveur :

Le choix de l'architecture Client/Serveur offre une grande souplesse et une évolution indispensable à l'entreprise, il n'en reste pas moins que les coûts induits par cette architecture sont très lourds.

Avec un Intranet, il n'est plus nécessaire de diffuser les applications, celles-ci sont programmées en HTML et/ou en JavaScript et/ou en Java et sont concentrées sur le serveur, ce recentrage fait des serveurs web les plaques tournantes du système.

### a3) Offrir un client universel :

Le client universel permet de ne mettre en place qu'une seule application pour accéder à l'ensemble des services existants ou à venir du système : messagerie, forums, transfert de fichiers, interrogations de bases données, applications, etc.

Cette approche est une évolution majeure de l'informatique de l'entreprise car elle permet plus de réactivité, plus de souplesse, tout en réduisant les coûts et les contraintes de déploiement.

### a4) Orienter l'Intranet vers la communication :

L'approche choisie ces vingt dernières années dans la construction des systèmes cause une dispersion de l'informatique. Les systèmes ont été construit autour des traitements (gestion de la production, analyse des données, bureautique individuel, ...). La communication entre personnes et services n'était pas critique pour l'activité.

Mais, en construisant un Intranet, on recentre le système sur la communication. En intégrant la messagerie, forums et serveurs d'information, on recherche à améliorer la communication. Cette communication entre les différentes unités de l'organisation et à rendre l'accès à la richesse d'information à tout le monde.

## III.2. b) Les acteurs d'un projet Intranet :

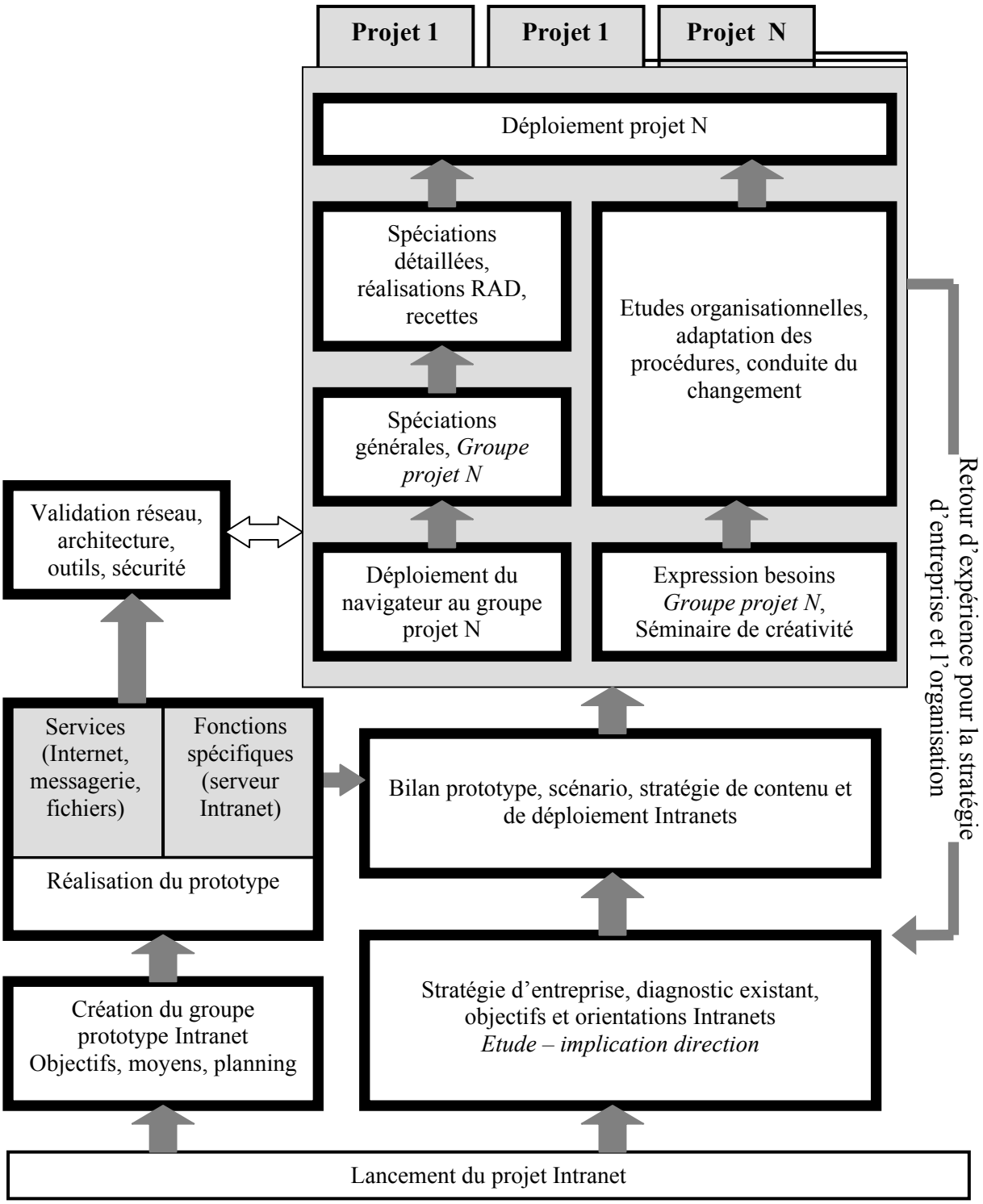
Le projet Intranet est mené par les hommes créatifs de l'entreprise, qui s'intéressent aux nouvelles technologies et qui ont les moyens de s'exprimer :

- Les chefs de projet (le chef et ses supérieurs).
- Les utilisateurs.
- Les animateurs.
- Les développeurs.
- L'administrateur de données.
- Le webmaster.

Il est aussi important de mettre en place un partenariat entre le maître d'ouvrage et le maître d'œuvre.

## III.2. c) Méthode de conduite d'un projet Intranet :

Un projet Intranet, par ses caractéristiques, par son objet et les techniques déployées, nécessite le déroulement de méthodes appropriées. Le schéma ci après permet de visualiser les différentes étapes nécessaires à la réussite de mise en œuvre d'un Intranet dans l'entreprise.




**Méthode de conduite du projet intranet**
**(Source : le projet Intranets)**

Ce schéma est à lire de préférence de bas en haut. Les interactions entre les différentes étapes sont très fortes. Le détaille des étapes est le suivant :

- **Stratégie et diagnostic :**

  Il est illusoire de se lancer dans la conception et la réalisation d'un réseau Intranet d'une certaine ampleur sans avoir une certaine idée de la stratégie de l'entreprise.

  Il est également clair que le projet Intranet ne pourra à lui seul déclencher les véritables mutation de l'organisation de l'entreprise. Il permettra de mettre en œuvre la volonté affirmée des décideurs et aura le mérite essentiel d'offrir à l'ensemble des collaborateurs de participer pleinement à la reconstruction de l'organisation.

  La phase du diagnostic doit permettre également d'identifier les contraintes internes et externes de l'entreprise sous les angles : fonctionnel, organisationnel, techniques et financier.

- **Scénario :**

  Le scénario est comparable à un petit schéma directeur de type opérationnel et orienté sur le fonctionnel et organisationnel. Le scénario débouche sur un découpage en sous-projet de conception et de réalisation sauf pour l'étude technique qui est faite pour l'ensemble des sous-projets.

- **Spécifications générales :**

  Après découpage fonctionnel et choix des projets prioritaires, le maître d'ouvrage et les utilisateurs doivent formaliser les spécifications fonctionnelles générales des nouvelles applications ou l'accès aux applications actuelles à maintenir.

- **Prototype :**

  Le prototypage a de nombreuses vertus. Il permet de valider les choix techniques, de présenter les premières fonctionnalités afin de faire émerger plus facilement le réel besoin des utilisateurs et il permet de mettre en place rapidement le navigateur et le serveur qui constitueront les fondations du futur Intranet. Le formalisme de cette phase sera très léger.

- **Expression du besoin :**

  Les séminaires d'expression des besoins se déroulent dans un délai d'une à deux semaines, lors de la première séance (1 à 2 heures), le prototype est présenté au groupe d'une dizaine d'utilisateurs de tous niveaux (dirigeants, cadres, techniciens, secrétaires,…).

  On y découvre les fonctions de messagerie, le serveurs web, les utilisateurs sont invités à l'accès à Internet, lors des séances suivantes, les utilisateurs sont invités à s'exprimer librement sur ce qu'ils ont vu, sur les besoins et souhaits que cela suscite en eux, sur les éventuelles difficultés.

- **Etudes d'organisation, conduite du changement :**

  Aucune des actions classiques de mise en organisation d'un projet ne doit être négligée dans le cadre dans le cadre d'un Intranet : mise à disposition des moyens nécessaires en postes de travail et outils de télécommunication sensibilisation, formation, organisation de la maintenance…

- **Etude technique :**

  Il s'agit de définir et mettre en place l'architecture technique nécessaire en élaborant l'architecture du réseau et la gestion du trafic, en choisissant les outils compte tenu de l'expérience du prototype.

- **Spécifications détaillées et réalisation :**

  Les développements peuvent être réaliser en démarches RAD (Rapid Appication Developement), en fusionnant les étapes de spécifications détaillées et réalisation, avec la collaboration active des utilisateurs.

- **Déploiement du navigateur et accès aux services Intranet :**

  Le déploiement du navigateur sur l'ensemble des postes capables de l'héberger permet aux utilisateurs de bénéficier très rapidement des fonctions de bases de l'Intranet (messagerie, forums, Internet,…). L'accès à Internet permet à chacun de se familiariser avec le navigateur et de découvrir l'étendue de la toile à l'échelle de la planète.

- **Retour d'expérience :**

  Le projet Intranet n'a pas vraiment de fin, au sens où l'une de ses caractéristiques réside dans sa forte capacité d'évolution. Les serveurs web doivent vivre, évoluer, s'enrichir en permanence. L'ouverture vers les clients ou fournisseurs aux partenaires de l'entre prise demande des adaptations et offre des nouvelles perspectives.

  En plus, les utilisateurs, principaux bénéficiaires de l'architecture, auront de nouvelles idées pour mieux travailler ensemble, mieux répondre aux, mieux forger la culture d'entreprise.

# III. 3) La mise en œuvre d'un site web :

## III.3. a) Préparation du cahier de charge pour le site :

### a1) Présentation de l'entreprise (résulte de l'état de l'existant) :

La présentation de l'entreprise doit contenir une description précise des informations suivantes afin de facilité la conception des propositions sur le fond du site afin qu'il soit bien adapté à l'image de l'entreprise :

- Activités, structures (humaines, financières,…).
- Produits, services.
- Objectifs généraux, environnement, concurrence, enjeux.
- Organisation de l'entreprise.
- Formes de communication.

- Le système d'information :
  - Moyens techniques (informatiques, numériques, …).
  - Information disponible (forme, format, …).
  - Circulation de l'information.

## a2) Le projet de serveur (résulte de l'analyse des besoins) :

- Objectifs :
  - Objectifs commerciaux, stratégiques.
  - Priorités, contraintes (ce qu'on veut… et ce qu'on ne veut pas).
  - Types d'informations présentées.
  - Services proposés.

- Cible :
  - Espace géographie (situation, langues, …).
  - Client final.
  - Distributeur.
  - Fournisseur - partenaire - ...

- Compétences disponibles - encadrement du projet.
- Planning prévisionnel.

## a3) Demande d'offres de prix :

Cette partie est très importante pour la formalisation et la forme du site et de son contenu ainsi que sa bonne marche sur le web et que pour son succès. Et finalement, pour qu'il puisse atteindre l'objectif fixé :

- Devis pour (en fonction des besoins) :
  - Etude et analyse, cahier des charges définitif.
  - Définition de la charte graphique et du contenu, conseil en communication, ...
  - Développements techniques (HTML, Base de données, Formulaire, Modules applicatifs,…).
  - Système de paiement électronique (pour commerce).
  - Numérisation, saisie, traductions, prises de vue ou de son, ….
  - Recherche bibliographiques, recherche concurrentielle sur Internet, ....
  - Achat , gestion d'un ou plusieurs nom (s) de domaine "nom(s) à définir".
  - Hébergement du site, mise en œuvre d'un service d'E-Mail (n adresses) et/ou d'un service FTP.
  - Système de paiement électronique.
  - Référencement du site (préciser méthode, nombre de moteurs et annuaires concernés, suivi périodicité).
  - Méthodes et procédures de transfert des données pour mise à jour du site (précision de volumes).
  - Formation et /ou transfert de compétences.

- Le(s) prestataire(s) doit fournir :
  - Informations générales sur l'entreprise.
  - Références (si possible sur un projet proche).
  - Moyens techniques.
  - Méthodes de travail.

## III.3. b) Conception et Démarrage du site :

### b1) Choisir le Nom de Domaine :

- Définir un Nom de Domaine : Un nom de domaine est une appellation affectée à une machine parce que les valeurs numériques sont peu conviviales. L'identification d'un ordinateur au moyen d'un tel nom doit être sûre, aussi un système hiérarchisé de classification est établi sous le nom de DNS (Domain Name Server). Différents types de domaines existent sur Internet.

| Suffixe | Dénomination |
|---|---|
| .fr | Entreprise française |
| .tm.fr | Marque déposée |
| .gou.fr | Ministère |
| .asso.fr | Association |
| .com | Domaine commercial international |
| .org | Organisation non gouvernementale |
| .edu | Université, école… |
| .gov | Organisation gouvernementale |
| .us | Entreprise américaine |

- Vérifier que le Nom de Domaine n'est pas déjà attribué.
- Choisir ".fr" ou ".com".
- Choisir un Nom de Domaine dure.

### b2) Choisir une solution d'Hébergement :

Dans notre choix, on doit se baser sur les points suivant :

- Hébergement interne ou externe (chez un prestataire).
- Plate-forme.
- Accessibilité.
- Statistiques.
- Coûts nécessaires.

### b3) Ergonomie :

- **Concevoir des pages graphies attrayantes et faciles à consulter :**

Pour allier la richesse des images et la rapidité, il faut employer correctement les formats graphiques et les palettes de couleurs. Il est par conséquent indispensable de les optimiser afin de limiter les temps de chargement. Le choix du format approprié, qui passe par bonne maîtrise de ses caractéristiques, permet également de comprimer considérablement la taille des fichiers.

- Choisir le format le plus économique : Deux formats sont actuellement supportés par tous les navigateurs, le GIF et le JPEG.

- Contourner l'incompatibilité des palettes de couleurs : Il convient donc de convertir les valeurs RVB (Rouge - Vert - Bleu) en valeurs hexadécimales : ainsi R=255, V=255 et B= 255 devient #FFFFFF.

- Utilisation d'images animées.

- **Normaliser les pages web avec les Feuilles de Style (CSS) :**

Le W3C à homologué une série de balises et d'attributs, afin de contrôler l'affichage des pages web. Il est donc désormais possible de paramètrer le texte avec des feuilles de style.

- Contrôler la typographie.
- Gérer les marges et les espacements.
- Possibilité de contrôler tous les styles d'un web par un fichier unique.

- **Possibilité de créer des illustrations et des animations Shockwave :**

La gamme de logiciels Macromedia permet de développer animations et illustrations ou de réutiliser des applications existantes pour rendre un site Web plus attrayant. L'utilisation a besoin du plug-in Shockwave.

## b4) Développement :

- **Concevoir des Formulaires HTML interactifs :**

Un formulaire HTML permet d'établir un dialogue pour rassembler des information sur les utilisateurs et les traiter directement, soit pour enrichir une base de données, soit pour les renvoyer vers un CGI.

Réservation de places, inscriptions, demandes d'information, achats en ligne… Le formulaire est indispensable à un site Web qui se veut plus qu'une simple vitrine. Ainsi, il est possible de passer de la consultation passive à un vrai dialogue, faisant remonter l'information depuis le visiteur jusqu'au propriétaire du site.

Le formulaire apporte l'organisation nécessaire à un traitement de l'information automatique et à grande échelle, en structurant les pages grâce à des champs de saisie formatés.

Pour créer un formulaire convenable il faut :

- Définir des zones de saisie conforment aux informations.
- Insérer des cases à cocher.
- Permettre de choisir en cliquant parmi des options.
- Etablir une liste de choix prédéfinis que l'utilisateur sélectionnera.
- Prévoir la possibilité pour l'utilisateur d'effacer toutes les données saisies.

On peut aussi utiliser le langage JavaScript pour réaliser des formulaires en le combinant avec HTML pour avoir des formulaires plus dynamiques.

- **Utilisation de JavaScript :**

On peut aussi utiliser le langage JavaScript pour réaliser des formulaires en le combinant avec HTML pour avoir des formulaires plus dynamiques ainsi que des pages plus actives et plus attractives.

- **Utilisation de JAVA :**

L'utilisation du langage JAVA a travers des applets autonomes qui s'exécutent dans les navigateurs des clients permet d'aller encore plus loin dans l'aspect dynamique et dans l'attractives vu la richesse de ces apports. Il nous permet aussi de concevoir des interfaces universelles pour toutes les plates formes.

- **La technologie ASP :**

L'utilisation de la technologie Active Server Pages permet de d'insérer des scripts ASP facilitant l'envoi d'information à l'utilisateur et la nouvelle directement de pages, afin de contrôler l'accès au serveur web.

Il est parfois nécessaire d'afficher plusieurs images lourdes. Plutôt que de les afficher toutes systématiquement, et que le changement de la page soit long, un formulaire permet d'afficher uniquement les images désirées.

- **Utilisation des ActiveX :**

Un document ActiveX est une application exécutable dans un conteneur tel que le navigateur. C'est un objet pouvant contenir d'autres ActiveX, des méthodes, ou des contrôles (boutons, zones de texte, liste, etc.). Les fichiers ActiveX compilé est placé sur un serveur HTTP et distribué sur Internet. Les utilisateurs lance sur leur poste depuis le navigateur, qui installe les composants et exécute l'ActiveX.

## b5) Référencent :

Promouvoir son site sur le web, c'est l'inscrire sur les serveurs de recherche. Si l'opération est réussie, un utilisateur pourra rapidement le trouver grâce à des mots clés.

- Se faire référencer par l'intermédiaire de sites de promotion. L'entreprise référence son site soit en s'adressant au serveurs (Yahoo, Lycos, Altavista, Ecila, Lokace, …), soit en confiant la promotion à au forunisseur d'accès. Le prix moyen en France est de 8 000 Frs. Cela peut atteindre 15 000 Frs en fonction du nombre de références demandées.

- Donner au site un titre décrivant l'activité.

- Trouver les mots-clés porteurs.

- Donner un complément d'informations par communiqué de presse.

- Choisir la bonne catégorie.

- Utiliser les Méta-tags.

- Utiliser les sites des bandeaux publicitaires.

## b6) Administration et Maintenance :

### Analyse de la fréquentation et la consultation du site web :

Les logiciels de statistiques analyses les informations des fichiers logs. Ces données permettent d'avoir. Cette analyse nous permettre :

- Au niveau de la fréquentation :
  - Connaître le nombre de fichiers ouvert par l'utilisateur.
  - Dénombrer les visites.
  - Savoir combien de requêtes ont été effectuées.
  - Evaluer le nombre de visiteurs.
  - Situer l'origine des utilisateurs (par pays, par fournisseur).
  - Cerner les pics de fréquentation.

- Au niveau de la consultation :
  - Etablir un classement de la consultation des pages.
  - Mesurer l'intérêt pour le site grâce au nombre de formulaires renvoyés.
  - Identifier la cause des erreurs techniques.

- Au niveau de l'amélioration :

  Une basse fréquentation sur un fichier peut avoir des causes multiples : manque d'intérêt pour le produit, rubrique dans une arborescence trop complexe, page précédente trop lourde à afficher en raison images trop nombreuses. Evidemment, il ne s'agit pas de remanier complètement le site mais de l'affiner par petites touches successives pour améliorer la fréquentation des fichiers délaissés.

## b7) Sécurité :

- Bien ajuster les paramètres du système.
- Utiliser un simulateur d'attaque.
- Analyser les fichiers logs.
- Tester les mots de passe.
- Sensibiliser les utilisateurs.
- Adopter une bonne stratégie de codification des mots de passe.
- Protéger les fichiers sensibles.
- Analyser les droits d'accès aux fichiers sensibles.
- Contrôler l'accès au réseau.
- Pré-définir les groupes d'utilisateurs.
- Protéger le serveur avec un Firewall (coupe-feu).

# IV) La sécurisation des transactions ?

La sécurité est un sujet très large, qui présente divers aspects. Sous sa forme la plus simple, elle doit permettre d'être sûr qu'un individu mal intentionné ne viendra pas lire des messages qui ne lui sont pas destinés, pire encore, les modifier. On peut aussi vouloir empêcher les accès non autorisés à des services en ligne et être sûr que, lorsqu'on reçoit des impôts un message se terminant par "A payer avant le vendredi dernier délai", ce message provient bien des services fiscaux et pas de la mafia. La sécurité doit également permettre de débusquer les captures et les rejets d'échanges légitimes, de même qu'elle doit empêcher un participant à une transaction denier sa réalité.

Les problèmes de sécurité des réseaux et des transactions peuvent être, en première approximation classée en quatre catégories : la confidentialité, l'authentification, la non - répudiation et le contrôle d'intégrité. La cryptographie permet la mise en œuvre des services de sécurité ci-dessous, qui ont pour objectif de protéger des données ou des transactions sous forme électronique.

- **Intégrité des données :** Le contrôle de l'intégrité d'une donnée consiste à s'assurer que cette donnée n'a pas été altérée accidentellement ou frauduleusement. Le plus souvent le contrôle de l'intégrité ne s'appuie pas à proprement parler sur un outil de cryptographie car son calcul ne requiert pas de convention secrète. Le contrôle d'intégrité passe par la question «comment être sûr que le message que l'on reçoit est bien celui qui a été envoyé et qu'il n'a donc pas été altéré en cours de route ? ».

- **Authentification :** elle nous permet de chercher à avoir la certitude que l'entité avec laquelle on dialogue est bien celles que l'on croit. Elle peut être de deux natures :
    - authentification des partenaires.
    - authentification de l'origine des informations.

  En pratique, ce service permet principalement de s'assurer que le correspondant connecté est bien le correspondant annoncé ou de s'assurer du signataire de l'acte.

- **Non-répudiation :** La non–répudiation permet d'obtenir la preuve de l'émission d'une information ou la preuve de sa réception. L'émetteur ou le récepteur ne peut ainsi en nier l'envoi ou la réception. Elle concerne les signatures, comment prouver qu'un client a bien passé électroniquement une commande de dix millions de scoubidous à 89 centimes pièces alors qu'il prétend que le prix était de 69 centimes seulement ?.

- **Confidentialité :** La confidentialité permet de rendre la lecture de l'information inintelligible à des tiers non autorisés lors de sa conservation ou surtout de son de transfert. Le chiffrement des informations constitue la technique la plus utilisée pour répondre à ce service. Elle rend compte du fait que seuls les utilisateurs habilités doivent pouvoir prendre connaissance de l'information, c'est souvent ce à quoi on pense premier lorsqu'on parle de sécurité.

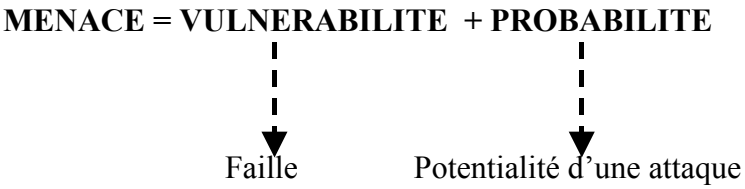
- **Signature numérique :** La signature numérique est une technique qui permet la mise en œuvre à la fois de l'intégrité des données, de l'authentification et de la non répudiation.

# IV. 1) Les Problèmes de Sécurités ? :

## IV.1. a) Les menaces :

Les menaces qui autrefois n'étaient que locales peuvent maintenant concerner tout un réseau d'entreprise. Il y a beaucoup de menaces contre lesquelles on doit se protéger quand on se connecte sur Internet, mais on peut les regrouper en quelques catégories générales :

- Les menaces contre le réseau interne.
- Les menaces contre les serveurs Internet.
- Les menaces contre la transmission des données (la confidentialité et l'intégrité).
- Les menaces contre la disponibilité des machines du réseau.
- Les menaces de répudiation.




Une Menace implique un risque

De façon quelque peu arbitraire, on peut regrouper de façon plus évidente les menaces potentielles en cinq grandes catégories personnalisées :

- **Classe 1 :** *Espion occasionnels* ne possédants pas de capacités en chiffrement mais ayant un succès physique à l'information cryptée.

- **Classe 2 :** *Hackers* agissant seuls ou petits groupe en mesure d'utiliser les programmes et techniques d'analyse cryptographique disponibles sur les messageries électroniques et possédant des ressources en matériel comparables à celles d'un bureau rempli de stations de travail.

- **Classe 3 :** *Pirates informatiques organisés ou organisation de taille moyennes* ayant une connaissance parfaite de toutes les techniques d'analyses cryptographique répandues dans le domaine public et qui sont en mesure de réunir des ressources matérielles d'environ un millier de stations de travail.

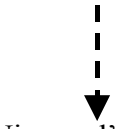
- **Classe 4 :** *Agences gouvernementales petites ou moyennes et grandes multination-ales* possédant une maîtrise parfaite de toutes les techniques publiques d'analyse cryptographie, mais aussi certaines connaissances et techniques confidentielles. Ces entités peuvent construire des engins d'analyse cryptographique utilisant des dizaines de milliers de circuits intégrés partiellement spécialisés.

- **Classe 5 :** *Grandes agences gouvernementales* possédant une maîtrise parfaite de toutes les techniques publique publiques d'analyse cryptographique, mais, aussi de

toutes les connaissances et techniques confidentielles. Elles peuvent capter l'ensemble des communications qui transitent par leur territoire (et éventuellement celui d'autres pays) et ont un accès prioritaire à des chaînes de fabrication de semi-conducteurs qui leur permettent de mettre au point et d'utiliser des millions des circuits intégrer spécialisés.

## IV.1. b) Les risques :

**RISQUE = SENSIBILITE + MENACE**



Niveau d'importance
d'une information

Un Risque est associé à une ressource

Un des risques que vous encourez en travaillant avec Internet est représenté par les célèbres pirates informatiques. La taille énorme du réseau d'Internet touche sa fiabilité et ouvre la porte aux problèmes suivants : erreurs de routage, pannes de transmission, corruption de données et pannes de composants physiques (comme les routeurs) et ce en n'importe quel des points en nombre apparemment infini.

Quelques risques existant sur le réseau sont :

- On peut voler votre mot de passe quand vous vous connectez à d'autres systèmes.
- On peut enregistrer vos lignes de communication et compromettre vos secrets industriels.
- On peut pénétrer vos systèmes et pirater vos comptes.
- On peut saturer votre réseau et provoquez une panne.

Puis viennent les risques légaux :

- On peut voler votre patrimoine intellectuel.
- On peut violer vos droits d'auteur et vos brevets.
- Vous pouvez ne pas respecter les contrôles à l'exportation des technologies.
- On peut mettre vos documents confidentiels sur des babillards publics.
- Vos employés peuvent être surpris à charger des fichiers pornographiques

Enfin les risques financiers et liés au commerce électronique :

- On peut modifier vos rapports et actes financiers.
- On peut détourner vos fonds.
- On peut fabriquer de la fausse monnaie.
- On peut se faire passer pour vous et effectuer des transactions financières à votre place.

## IV.1. c) Les attaques :

### ATTAQUE = RÉALISATION D'UNE MENACE

Certaines attaques, comme le trucage d'adresse, ont reçu une grande attention, il est important de garder à l'esprit que ce type d'attaques ne sont que l'un des nombreux types d'attaques observées sur Internet. Les différents types d'attaques possibles sont :

- **Les attaques fondées sur les mots de passe :**

  Les attaques sur les mots de passe impliquent une certaine exploitation des mots de passe. Une méthode commune d'infiltration pour intrus est d'essayer une combinaison nom d'utilisateur – mot de passe, puis une autre, ainsi de suite, jusqu'à ce que qu'une combinaison particulière le connecte à un système.

- **Les attaques qui exploitent un accès par confiance :**

  Plusieurs systèmes d'exploitation (UNIX , VMS ET Windows NT) ont des mécanismes d'accès sûrs conçus pour faciliter l'accès à d'autres systèmes ou domaines. Un agresseur qui devine le nom d'une machine ou une combinaison utilisateur – nom de machine peut accéder à une machine qui permet cet accès sûr.

  La menace d'accès machine par la confiance non autorisée augmente encore d'avantage quand le mécanisme de "confiance réciproque" ou confiance commune entre deux machines, existe. Un agresseur a seulement besoin d'accéder à une machine pour être capable d'accéder à l'autre.

  La limitation forte (ou dans certain cas l'interdiction) des mécanismes de confiance réciproque et la transmission de la confiance diminue les risques de sécurité sur Internet de façon substantielle.

- **Les attaques basées sur le trucage IP :**

  Le trucage consiste en la fourniture d'informations fausses sur une personne ou sur l'identité de la machine d'origine pour obtenir un accès non autorisé aux systèmes et aux services qu'il fournit. Le trucage exploite la manière dont un client et un serveur se connectent l'un à l'autre. Bien que le trucage puisse se produire avec de nombreux protocoles différents, le trucage IP est l'attaque par trucage la plus connue de toutes.

  La première étape dans une attaque de trucage est d'identifier deux machines cibles, que nous appellerons A et B. une fois que les systèmes cibles sont identifiés, l'agresseur essaiera d'établir une communication avec la machine B de telle façon que B croie qu'elle a une communication avec A, alors qu'en réalité la communication est avec la machine de l'agresseur, ceci est fait en créant un message truqué.

Le trucage IP est lourd et pénible. Cependant, une analyse récente d'incidents à découvert des outils automatiques qui réalisaient l'attaque complète par trucage en moins de 20 secondes. Le trucage IP est une menace dangereuse et croissante, mais heureusement relativement facile à contrer. La meilleur défense contre le trucage est de configurer des routeurs pour rejeter tout paquet entrant qui prétendrait venir du réseau interne. Cette précaution simple empêchera toute machine externe d'utiliser les relations de confiance établies sur le réseau interne.

- **Les attaques basées sur le détournement de session :**

Dans le détournement de session, un intrus cherche une communication réelle entre de machine et essai de prendre le pouvoir. Après avoir pris le contrôle d'une machine (Firewall ou un composant d'un réseau) 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.

Après avoir vu la communication, l'intrus peut générer le trafic qui lui semble venir de l'une ou l'autre des deux machines, en volant effectivement la session de l'un des deux correspondants. L'intrus obtient ainsi les mêmes privilèges d'accès que l'utilisateur légitime. Ensuite, l'utilisateur légitime est éliminé de la communication et l'intrus peut maintenant continuer ce que l'utilisateur originel a commencé.

Se protéger contre le détournement de session est extrêmement difficile. Même les mécanismes d'authentification les plus forts ne réussissent pas toujours à empêcher les attaques.

- **Les attaques basées sur l'observation du réseau/l'examen des paquets :**

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. Les réseaux à supports partagé présentent un risque particulier car les paquets peuvent être captés à tout point de ces réseaux sauf si certains dispositifs de sécurité spéciaux sont mis en place. La capture des paquets de cette manière est connue comme "observation du réseau".

Si un renifleur est installé n'importe où sur le long chemin entre machine origine et machine destination dans n'importe quel réseau d'entreprise, les informations de connexion peuvent être saisies et utilisées ensuite pour attaqué la machine de destination.

L'observation du réseau est une des menaces les plus sérieuses pour les entreprises, même si les réseaux internes ne sont pas connectés à Internet. Cette méthode d'attaque est utile non seulement pour capturer les informations de connexion, mais, encore pour obtenir illégalement les données d'une entreprise et ses messages électroniques. De plus, il n'est pas aussi facile de se défendre contre l'observation du réseau comme il pourrait le sembler.

Les mesures contre l'observation du réseau :

- L'authentification forte.
- L'inspection physique du réseau.
- La technologie des répétiteurs de paire torsadée.
- L'examen systématique.
- La politique (l'interdiction de renifleur, …).
- Le chiffrement du réseau.

- **Les attaques qui utilisent la vulnérabilités techniques :**

Les nombreuses vulnérabilités qui sont typiquement utilisées pour obtenir des services TCP/IP existent dans des programmes comme *sendmail*, FTP serveurs et les programmes NFS et NIS.

Ces vulnérabilités peuvent être exploitées pour permettre beaucoup d'actions non autorisées, comme l'utilisation de ces services, l'accès aux fichiers critiques, l'accès aux données des utilisateurs et/ou des programmes et accès privilégié. Les fournisseurs réparent souvent ces vulnérabilités, uniquement pour découvrir qu'un autre utilisateur d'Internet "un cracker" a trouvé un autre moyen pour compromettre un ou plusieurs de ces services rendant nécessaires encore une réparation..

- **Les attaques qui utilisent les bibliothèques partagées :**

Les programmes dans UNIX et dans d'autres systèmes lisent souvent des bibliothèques partagées pour s'exécuter. Les intrus ont un astuce fréquent : ils remplacent certains programmes dans les bibliothèques partagées par des programmes qui accomplissent choses avantageuses pour eux.

Remplacer un programmes dans une bibliothèque partagée par autre avec d'autres caractéristiques permet, par exemple, à intrus d'avoir un accès privilégié en exécutant un programme qui appelle cette bibliothèque partagée. La meilleure méthode pour contrer cette vulnérabilité est généralement de contrôler et d'assurer l'intégralité des bibliothèques partagées sur chaque système.

## IV.1. d) Les adversaires :

De nombreux problèmes de sécurité sont dus à des individus malintentionnés. Le tableau ci-dessous en donne quelques exemples. On doit bien comprendre que pour qu'un réseau soit sûr il ne suffit pas que ses logiciels soient sans erreurs, il faut aussi se montrer plus malin que des adversaires intelligents et décidés, qui parfois disposent de gros moyens. Il faut aussi comprendre que certaines mesures arrêtant des adversaires occasionnels auront peu d'effets sur d'autres, plus motivés.

| Adversaire | But recherché |
|---|---|
| Etudiant | S'amuser à lire le courrier électronique des gens |
| Pirate | Tester le système de sécurité et/ou voler des données |
| V.R.P. | Prétendre avoir l'exclusivité sur la France et pas seulement sur l'Ardèche |
| Homme d'affaire | Connaître le plan média de son concurrent |
| Ex - employé | Se venger d'un licenciement |
| Comptable | Détourner de l'argent |
| Agent de change | Renier une promesse faite par courrier électronique |
| Escroc | Voler des numéro et des codes de cartes de paiement |
| Espion | Connaître le potentiel militaire de l'ennemi |
| Terroriste | Voler des informations secrètes concernant la guerre bactériologique |

# IV. 2) Les Solutions :

## IV.2. a) L'Authentification et les signatures digitales :

L'authentification consiste à signer et vérifier le contenu des documents. Le moyen le plus simple d'arriver à ce résultat est de couper la présentation binaire du document en morceaux, puis d'additionner tous les morceaux comme s'ils étaient des nombres. Les algorithmes de "Broyage ou Hashing" servent à signer des documents en les plongent dans une potion magique cryptographique destinée à gêner les personnes cherchant à savoir comment un changement apporté au document affecte le broyage Cette technique empêche les pirates de modifier un document en gardant intacte la valeur de broyage.

Les bits obtenus sont alors chiffrés avec la clé privée du signataire et la chaîne nouvelle créée est transmise en même temps que le document. Le destinataire broie le document reçu, déchiffre la signature et compare les deux résultats. S'ils correspondent, le destinataire est à la fois certaine de la provenance du document et de son intégrité.

Mais cette théorie comporte deux failles. Elle suppose d'abord que la clé privé de l'expéditeurs n'a pas été découverte. Celui-ci doit toujours avoir un œil sur elle. Deuxièmement, la théorie suppose que le destinataire possède une copie valide de la clé publique de l'expéditeur. Si des personnes malintentionnées dérobent une clé privée quelconque ou se cachent derrière une fausse clé publique, ils peuvent construire une signature appartenant correcte. Ce problème n'est pas propre aux signatures numériques : la gestion des clés est le point le plus délicat de la cryptographie pratique.

### a1) Les Masque jetable :

Qu'est ce qu'un masque jetable ? vous disposez, avec votre correspondant, d'un grands nombre de bits choisis au hasard. Vous appliquez aux bits de votre message un traitement **xor** avec une chaîne de bits aléatoires aussi longue que le message. Vous envoyez le résultat à votre correspondant, avec un en-tête de bits précisant quels bits ont été utilisés. Il applique un **xor** au message chiffré avec la même chaîne de bits aléatoires et le texte originel apparaît comme par magie.

Le masque jetable ne nécessite pas que les bits soient complètement aléatoires, ils doivent juste être suffisamment imprévisibles pour qu'un adversaire ne puisse retrouver l'information d'origine à partir des chiffrées. Si on utilise les masque correctement, ils permettront de nous protégés contre les ***Menaces de Classe 5***.

Mais les masques jetables comporte quelques problèmes :

- Il faut trouver le moyen de communiquer l'ensemble de bits à son correspondant avant de communiquer
- Il ne faut pas jamais utiliser la même chaîne de bits deux fois de suite.
- Il faut veiller sans arrêt sur son masque.

## a2) Les Mots de passe :

Un mauvais mot de passe peut rendre vos données presque aussi vulnérables que si elles n'étaient pas protégées du tout. Le mot de passe le plus courant est celui qu'on utilise pour se connecter à son compte. Comme la plupart de ces mots de passe sont trop simples à trouver, le *login* est l'un des chemins d'accès pour les *Hackers*.

- **Qu'est ce qu'un mauvais mot de passe ? :**

Un mauvais mot de passe, c'est souvent :

- Un nom propre..
- Un nom commun.
- Une variante de votre *login* utilisateur (ex : le *login* à l'envers).
- Une date d'anniversaire.
- Le même caractère répété plusieurs fois (ex : hhhhhhhh).
- Un mot de passe récupéré dans un article sur "les bons mots de passe".
- Un mot de passe par défaut fourni par l'ordinateur (ex : "nisplus" dans le cas d'Unix).

- **Qu'est ce qu'un bon mot de passe ? :**

Un bon mot de passe doit comporter assez d'éléments aléatoires pour être sûr, mais rester mémorisable. Ce sera par exemple :

- Un couple de mots sans rapport choisis au hasard, de préférence séparés par un caractère spécial ou un chiffre (ex : capitalisme#football).
- Une chaîne d'au moins huit caractères, relativement facile à prononcer mais sans aucun sens (ex : merdadouch). Certain programmes savent générer ce type de mots de passe.
- Une chaîne aléatoire au format des plaques d'immatriculation françaises (ex : 75SDF1234). Mais, n'utilisez jamais le numéro de votre voiture.
- Des initiales suivies d'un numéro de téléphone choisi au hasard dans l'annuaire (ex : AF0231425364).

## a3) La signature des messages :

PGP a d'autres fonctionnalités que le chiffrement des messages, on peut aussi l'utiliser pour signer électroniquement un document avec sa clé privée. Cela veut dire que vous pouvez

envoyez un message que n'importe qui peut lire, mais en étant sûr qu'il vient de vous. Une signature électronique ne peut être imitée et un document signé ne peut être modifié sans invalider la signature. Ainsi, une signature ne sert pas uniquement à authentifier des données mais aussi à les protéger de toute altération.

## IV.2. b) Les Algorithmes et les Outils de Cryptage et de Chiffrement :

L'ensemble des algorithmes de cryptage utilises des algorithmes à de chiffrement soit à clé secrète soit à clé publique ou les deux en même temps.

Un système de chiffrement **à clé secrète** ou **symétrique**, repose sur le partage entre deux interlocuteurs en communication, d'une même clé secrète utilisée à la fois pour le chiffrement d'un message et pour son déchiffrement. La clé devra être échanger au préalable en toute sécurité.

Un système de chiffrement **à clé publique** nécessite que :

- Chaque utilisateur possède son propre couple de clés différentes *S* et *P*.
- La clé *S* est gardée secrète par son propriétaire qui l'utilise pour sa propre procédure de déchiffrement des messages reçus ou de signature de messages.
- La clé *P*, dérivée de la clé *S* par une fonction à sens unique (c'est à dire par une fonction facilement calculable mais dont l'inversion est extrêmement difficile), est rendue publique.

Ainsi, pour chaque système de chiffrement à clé publique, le choix d'un couple de clés *S* et *P* et la publication de la clé publique *P* par un utilisateur souhaitant recevoir des messages ou émettre des signatures, permettent à tout autre utilisateur de lui envoyer des messages chiffrés ou de vérifier ses signatures.

Une cette différence faite, regardons de près les solutions existantes pour les problèmes qui existent à ce sujet :

**rot13 :** c'est un chiffrement simple par substitution. Protège contre les ***Menaces de Classe 0*** : à recommander seulement au crime organisé.

**Crypt :** c'est un utilitaire UNIX est fondé sur une version simplifiée du code machine World War II. Les logiciels permettant de casser le code Crypt sont légion sur Internet. Protège contre les ***Menaces de Classe 1 seulement***.

**Chiffrement propriétaire dans certaines applications :** Les suites logicielles les plus connues vous permettent généralement de chiffrer les fichiers. Il s'agit de chiffrements propriétaires souvent aisés à forcer. Protège contre les ***Menaces de Classe 1 seulement***.

**Le DES :** Le DES, ou *Data Encryption Standard*, a été développée au début des années 1970 par IBM. C'est un système à clé symétrique. Les interlocuteurs désirant communiquer avec DES devront préalablement avoir échangé leurs clés secrètement. Il travaille en manipulant des extraits de 64 bits du document à chiffrer qu'il brouille 16 fois d'une façon particulière.

La seule faiblesse importante du DES réside dans la taille relativement courte de la clé de chiffrement : 56 bits. En moyenne, on trouve donc la bonne clé en deux heures. Utilisé avec une bonne clé, le DES convient aux ***Menaces de Classe 2***. On peut éventuellement l'étendre aux ***Menace de Classe 3*** pour encore quelques années.

**Le triple DES :** Le triple DES compense l'un des défauts principaux du DES : la taille réduite de sa clé de chiffrement. Comme son nom l'indique, le triple DES effectue trois passes DES sur le document à chiffrer. En utilisant des clés différentes à chaque étape, on peut obtenir un chiffrement avec une clé de 168 bits (3 x 56). Un grand nombre de spécialistes estiment que cette taille est trop importante, il utilisent donc le même clé pour les première et troisième étapes, ce qui permet d'obtenir finalement une clé de 112 bits. Ce dernier mode est parfois désigné sous le terme de DES-EDE (*Encode-Decode-Encode*). Protège contre les ***Menaces de Classe 3 et éventuellement de Classe 4***.

**IDEA :** L'IDEA, pour *International Data Encryption Algorithm*, a été développé à la fin des années 1980 par James L. Massey et Xuejia Lai à l'ETH de Zurich. Selon Zimmermann. Comme le DES, l'IDEA manipule des blocs de données de 64 bits à la fois, mais avec un algorithme différent et breveté. De manière plus importante, l'IDEA utilise des clés de 128 bits, assez longues pour résister à une recherche brutale qui testerait toutes les combinaisons possibles. IDEA est utilisé dans le programme de PGP. Il permet de protège contre les ***Menaces de Classe 3 et éventuellement de Classe 4***.

**RSA :** RSA est un système de chiffrement et d'authentification par clé publique. Dans le chiffrement à clé publique, on crée deux clés. L'une des deux clés, que l'on rend publique, est utilisée par quiconque souhaite vous envoyer un message secret. L'autre clé gardée secrète et utilisée pour déchiffrer le message. Pour répondre, on utilise la clé publique de l'expéditeur. L'intérêt de cette technologie est qu'elle permet de communiquer confidentiellement avec quelqu'un sans avoir à échanger des clés secrètes.

Avec RSA, on crée sa clé publique en multipliant deux nombres premiers de taille à peu près égale. La clé secrète est l'un des deux nombres premiers. On peut toujours retrouver l'autre en effectuant une division. Ainsi, une clé publique RSA de 512 bits est le produit de deux nombres premiers d'une taille de 256 bits chacun. Suivant la longueur de la clé, RSA contre les ***Menaces*** suivantes :

- ***512 bits : Classe 2.***
- ***768 bits : Classe 3.***
- ***1023 bits : Classe 4.***

**RIPEM :** PEM, *Privacy-Enhanced Mail*, est un standard Internet pour envoyer du courrier chiffré et/ou authentifié. PEM permet d'utiliser de multiples schémas de chiffrement et de signatures. RIPEM (*Riordan's Internet Privacy-Enhanced Mail*) est une implémentation de ce standard qui utilise DES pour le chiffrement et RSA pour la clé publique. En option RIPEM peut utiliser, au moment du chiffrement, le triple DES.

Comme dans le cas de RSA, la protection de RIPEM dépend de la taille de la clé utilisée et permet de contrer les ***Menaces*** suivantes :

- ***512 bits et DES : Classe 2.***
- ***768 bits et DES : Classe 3.***
- ***1023 bits et DES : Classe 4 (peut-être).***

**PGP :** Les héros sont nombreux sur Internet. Parmi tous eux, Philip Zimmermann représente une catégorie à lui seul. Il ne s'est pas contenté d'écrire un excellent programme, mais à risqué la prison pour prix de ses efforts. Le programme de Zimmermann s'appelle PGP, *Pretty Good Privacy*, et son concept est similaire à celui de RIPEM.

Comme RIPEM, PGP utilise la technique de clé publique de RSA mais IDEA à la place de DES pour le chiffrement. PGP systématise la distribution de clés publiques et dépasse RIPEM en maintenant secrète l'identité de l'expéditeur ce qui complique une l'analyse du trafic. La protection qu'offre PGP comme avec RSA qu'il utilise, dépend de la taille de la clé. Il permet de contrer les ***Menaces*** suivantes :

- ***512 bits : Classe 2.***
- ***768 bits : Classe 3.***

## RC2 et RC4 :

RC 2 et RC4 sont des algorithmes propriétaire développés par Ron Rivest, de RSA Data Sécurity.

RC 2 et RC4 avec des clés de 40 bits peuvent contrer ***les attaques Classe 1***. Ils fournissent aussi une protection à court terme (quelques jours) contre ***les attaques Classe 2***.

RC 2 et RC4 avec des clés plus longues (128 bits, par exemple) sont peut-être aussi efficaces que l'IDEA ou le triple DES, mais on n'est pas encore sûr. Il ne sont pas recommandés pour ***les menaces au-delà de la Classe 2***.

## b11) Clipper, Capston, Skipjack et Tessera :

Le socle sur lequel furent bâties de nombreuses applications commerciales – le DES – se fragilise rapidement, érodé par les vagues successives des avancées technologiques (dans les circuits intégrés). Les utilisateurs sont réticents pour adopter d'autres outils – IDEA, RCA4 et le triple DEA – sans l'accord du gouvernement américain. Pour résoudre ce dilemme, la NSA (*National Security Agency - USA*) a proposé une famille de produits de chiffrement à support matériel, aux noms de Clipper, Capstone, Skipjack et Tessera. Ces produits mettent en œuvre un nouveau concept appelé le ***Key escrow***.

Voici comment cela fonctionne. L'algorithme de chiffrement de Clipper, Skipjack, est secret : la NSA ne souhaite pas que le grand public connaisse ce qu'elle considère comme une méthode de chiffrement très efficace. Pour utiliser l'algorithme, les constructeurs doivent acheter une puce spéciale qui le contient sous une forme microcodée inviolable. Les utilisateurs peuvent choisir leurs propres clés de session de 80 bits. La puce chiffre cette clé de session avec une clé spéciale de 80 bits gravée dans le silicium au moment de sa construction. Chaque clé spéciale de puce est séparée en deux parties de 40 bits détenues par deux agents ***Key escrow*** distincts.

L'algorithme Skipjak étant secret on ignore son degré de sécurité ce qui nous amènes à dire que peut-être que la NSA a installé une porte secrète pour découvrir les clés et les messages. Clipper est efficace contre les ***Menaces de Classe 4.*** Il est aussi un bon allié contre les ***Menaces de Classe 5*** pourvu qu'elles n'émanent pas du gouvernement américain.

## b12) La Carte PCMCIA :

L'un des produits les intéressants dans le domaine de sécurité des données est la carte de chiffrement. Celle-ci contient une mémoire non-volatile, inviolable et une puce implémentant un ou plusieurs algorithme. Une carte PCMCIA (*Personal Computers Manufacturers Association and Computer-Industry Association*) a la taille d'une carte de crédit et est environ quatre fois plus épaisse.

Son intérêt réside dans le fait que votre clé ne doit jamais la quitter et certaines implémentations de cette technologie rendent virtuellement impossible de trouver la clé sur la carte. Quand vous voulez décoder un message reçu sur l'ordinateur, vous insérez la carte PCMCIA dans la baie. Vous tapez votre mot de passe, celle-ci est déverrouillée et l'ordinateur lui fournit alors la clé de session, chiffrée par l'émetteur avec votre clé publique. Le chiffrement fonctionne de la même manière.

Parmi les avantages de la carte de chiffrement :

- Il est facile de la garder sur soi.
- Si on vous la vole, on ne peut l'utiliser sans connaître votre mot de passe.
- Vous savez si elle est perdue ou volée.
- Certaines implémentations empêchent d'extraire de la carte la clé secrète, même avec le mot de passe.

L'un des désavantages de cette technique est qu'on ne peut pas effectuer de copie de sauvegarde de la carte. Dans la plus part des cas, le risque de perdre ses données, avec une carte de chiffrement, est plus grand que celui de se les faire dérober.

# IV.2. c) Les Firewalls :

Un Firewall (ou coupe-feu ou garde barrière) est presque toujours installé dans le but de protéger un réseau privé des intrusions illégitimes. Dans la plupart des cas, il sert à empêcher des utilisateurs non-autorisés d'accéder aux ressources de ce réseau et parfois à interdire une exportation frauduleuse d'informations. L'exportation d'informations passe parfois au second plan, mais, pour beaucoup d'entreprise c'est une préoccupation importante.

## c1) Les éléments constituants d'un Firewall :

On se trompe souvent de terminologie lorsqu'on parle des Firewalls car ils ont presque tous une implémentation voire un objectif différent :

**1) Le routeur-filtre :** le routeur-filtre est un élément de base de la plupart des Firewalls. Ce peut être un routeur commercial ou résidant au contraire dans l'organisation, qui possède des fonctions de filtrage. En général, ces routeurs peuvent bloquer le trafic entre des réseaux ou des hôtes spécifiques au niveau du port IP. Certains Firewalls ne sont rien de plus que des routeurs filtres installés entre un réseau privé et l'Internet.

**2) Le hôte bastion :** les bastions ou places fortes ont une vue d'ensemble sur toutes les zones avoisinantes et possèdent généralement des murs épais. Un hôte bastion est un système identifié par l'administrateur du Firewall comme un point renforcé de la sécurité du réseau. La plupart du temps, on accorde une attention particulière à leur solidité, on les inspecte régulièrement et ils sont parfois équipés logiciels modifiés.

**3) La double passerelle locale :** certains Firewalls ne disposent pas d'un routeur de protection, mais, d'un système à cheval sur le réseau privé et Internet, qui désactive le trafic direct TCP/IP. Les hôtes du réseau privé et ceux d'Internet peuvent communiquer avec la passerelle, mais, jamais directement entre eux. Une double passerelle locale est par définition un hôte bastion.

**4) La passerelle à hôte filtré :** est peut-être la configuration de Firewall la plus courante. On utilise pour l'implémenter, un routeur de filtrage et un hôte bastion qui la plupart du temps se trouve sur le réseau privé. Le routeur de filtrage est configuré de telle sorte que l'hôte bastion soit l'unique interlocuteur autorisé du trafic venant d'Internet. Tous ses ports, en outre, ne sont pas accessibles, ce qui limite le nombre de services autorisés.

**5) La sous-réseau filtre :** dans certains configurations de Firewalls, on crée et isole un sous-réseau entre Internet et le réseau privé. L'isolement s'effectue généralement par le biais de routeurs de filtrage. La plupart du temps, un sous-réseau filtré est configuré de telle sorte qu'Internet et le réseau-privé y aient tous deux accès, mais, sans pouvoir aller plus au-delà. Certaines implémentations de sous-réseaux comprennent un hôte bastion jouant le rôle d'un terminal ou supportant des passerelles pour applications.

**6) La passerelle d'applications :** ce type de passerelle est aussi appelée *proxy gateway*. La plupart des programmes Internet fonctionnent sur le mode stockage-redistribution, les logiciels de courrier et les news Usenet collectent des informations, les examinent et le redistribuent. Les passerelles d'applications sont des redistributions – ou réflecteurs – de services particuliers, qui opèrent généralement en mode utilisateur plutôt qu'en mode protocole. Ces redistributions, lorsqu'elles fonctionnent sur un Firewall, peuvent représenter une certaine menace pour la sécurité.

**7) La passerelle hybride :** Les passerelles hybrides entrent dans la catégorie "divers & bizarres" de la liste. C'est, par exemple, un hôte relié à l'Internet mais uniquement accessible via des liens séries connectées sur le serveur terminal Ethernet du réseau privé. De telles passerelles peuvent utiliser plusieurs protocoles en même temps ou les uns sur les autres. Les routeurs surveilleront toutes les connexions TCP/IP ou étudieront d'une manière ou d'une autre ou le trafic pour prévenir une attaque.

## c2) La mise en place d'un Firewall :

Même en considérant que les Firewalls remplissent leur mission d'aide à la protection du réseau, il reste important d'en examiner chaque type sous différents angles :

- Le contrôle de dégâts.
- Les zones à risque.
- Le contrôle des intrusions.
- La facilité d'utilisation.
- L'approche théorique.

## c3) Les limitations des Firewalls :

Contrairement à une idée reçue, les Firewalls ne sont pas la panacée pour vos problèmes de sécurité Internet. Il y a beaucoup de tâches que des Firewalls ne peuvent exécuter :

- Les Firewalls ne garantissent pas l'intégrité de données.
- Les Firewalls ne fournissent aucune authentification de l'origine des informations.
- Les Firewalls ne fournissent aucune confidentialité pour les informations.
- Les Firewalls ne protègent pas contre des menaces internes.
- Un Firewall est le seul point d'entrée d'un réseau.

### IV.2. d) IP nouvelle génération (IPng) :

La version actuelle du protocole Internet (IP) a atteint la fin de sa vie. Un remplacement proposé d'IP, connu comme IP nouvelle génération (IPng) est développée par l'IETF. Dans le domaine de la sécurité, IPng fournit les services d'intégrité, d'authentification et de confidentialité. Ces services peuvent être fournis ensemble ou isolément, en utilisant la même Entête d'Authentification (AH) et les méthodes d'Encapsulating Security Payload (ESP) comme elles sont proposées pour la version actuelle d'IP. La différence majeure est que l'Entête d'Authentification sera nécessaire dans IPng tandis que dans la version actuelle IP elle est un élément optionnel.

## IV. 3) La Mise en Œuvre de la Sécurité :

La sécurité parfaite est un but difficile à atteindre. En pratique, il faut tenir compte de toutes les menaces possibles et essayer de s'en prémunir de manière équilibrée en choisissant un plan de sécurité adapté à la situation. Pour ce faire, il va falloir répondre à un certain nombre de questions dont le détail est ci-après :

- **Quel type de données est-ce que je veux protéger ? :**
  Un grand nombre d'informations différentes méritent d'être protégées : fichiers médicaux, spécifications d'un produit nouveau, facture envoyée par courrier électronique, etc. Chaque type d'information requiert une approche spécifique.

- **Quelle quantité de données est concernée ? :**
  Un message E-Mail peut avoir une longueur de mille octets dont quelques douzaines, seulement, contiennent de l'informations à protéger. Une vidéoconférence sur un réseau de fibre optique peut, quant à elle, générer des centaines de gigaoctets par heure.

- **Combien de temps les données resteront sensibles ? :**
  Les discussions en petit comité sur un produit révolutionnaire ne doivent pas être protégées après annonces officielles à la presse. En revanche, l'infection d'un individu par le virus de SIDA peut être secrète tout au long de sa vie, voire après sa mort.

- **Quelle confiance puis-je avoir dans la source de mes données et dans leur destination ? :**
  La communication entraîne des risques particuliers. Des personnes mal intentionnées peuvent intercepter les messages en cours de route, pour les lire ou simplement connaître le nom du destinataire. Elles peuvent aussi modifier leurs contenus ou en écrire de nouveaux sous votre identité. Avec des degrés divers de réussite le chiffrement doit prendre en compte ces paramètres.

Mais les données sont également vulnérables sur le site où elles sont crées et sur celui où elles sont envoyées. La protection des informations sur un endroit fixe peut être encore plus difficile que la confidentialité de leur communication. On peut s'assurer, avec un peu d'attention, qu'on ne transmet que des données chiffrées, mais il faut bien déchiffrer de temps en temps les informations stockées sur des sites particuliers, si on veut les utiliser.

- **Combien de personnes partageront-elles les informations ? :**

Plus le nombre de personnes détenant un secret est grand, plus celui-ci est menacé. Les chiffres parlent :

- Si 10 personnes connaissent un secret et qu'on a la certitude que chacun d'entre eux à 99%, il y a 10% de chances que le secret soit divulgué.
- Si 100 personnes sont dans la confidence, il y a 63% de chances que quelqu'un parle.

Donc comment trouver le coupable dans une liste de suspects certainement innocents à 99% ?.

- **Contre qui dois-je protéger les données ? :**

Une bonne analyse des menaces est cruciale dans la mise en place d'un système de sécurité.

- Les curieux occasionnels.
- Les Hackers.
- Les espions industriels.
- Les agences gouvernementales spécialisées.

- **Quelles sont les conséquences d'une perte de confidentialité ? :**

Une liste de clients dérobée peut faire perdre des ventes à une entreprise. Plus les conséquences d'une perte de confidentialité sont graves, plus on doit veiller à protéger les données.

- **Ai-je l'obligation légale de protéger mes données ? :**

Dans certain cas la loi exige qu'on protège l'information. Parmi, les organismes qui veille au respect de cette loi en France, il y a la commission informatique et liberté.

- **A qui demander conseil en toute confiance ? :**

C'est l'un des problèmes les plus délicats. Pour résoudre ce problème on peut faire appel à un consultant ou à une entreprise spécialisée telle que la société ASCOM Tech AG (Suisse).

- **Quelles sont les autres façons frauduleuses pour accéder aux données ? :**

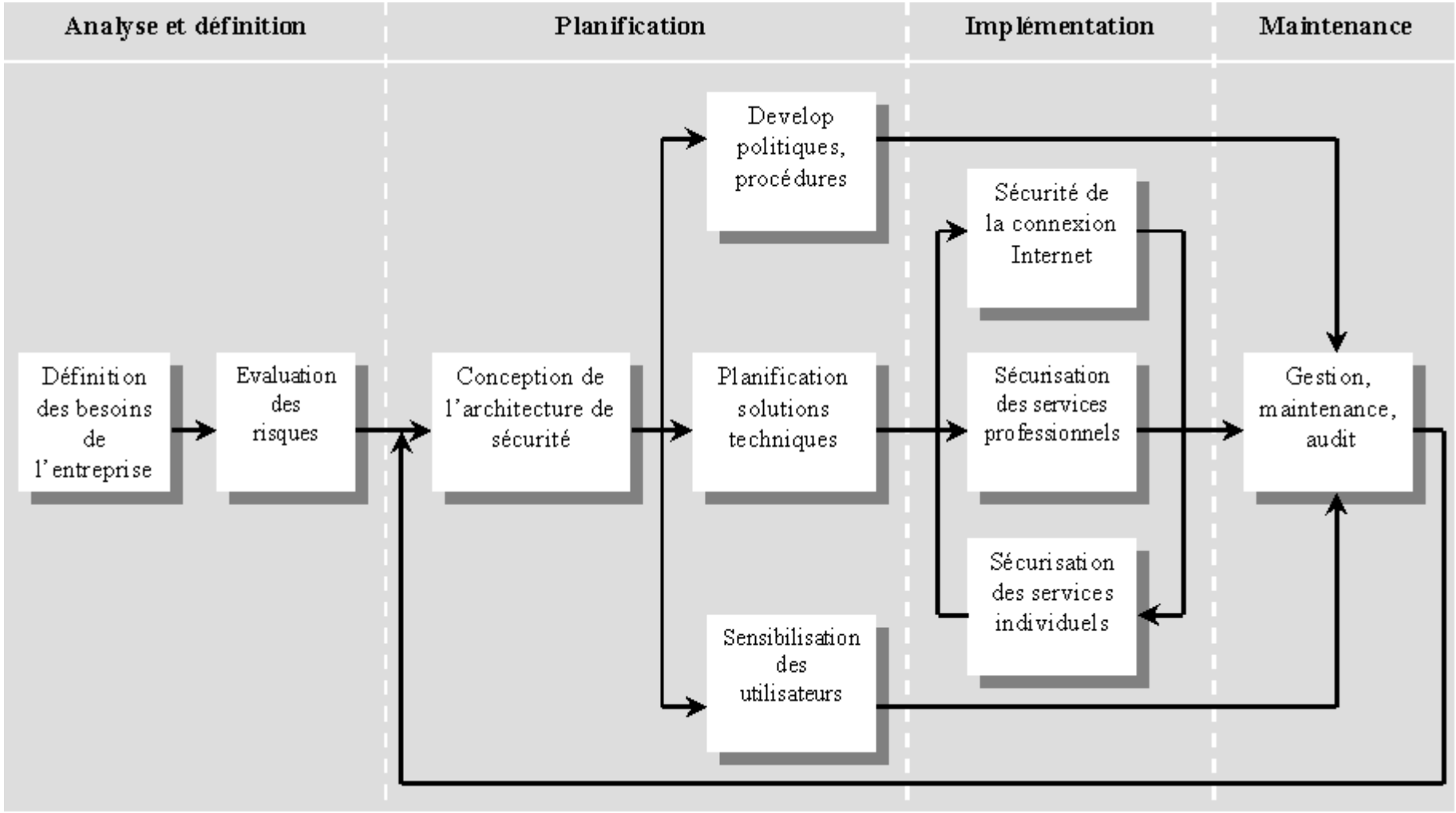
Un point important, en cryptographie, est de savoir distinguer le type de menaces auquel on a faire. Il faut absolument en tenir compte dans un système de sécurité bien conçu et s'en préoccuper avec autant de soin que du chiffrement des messages sur Internet.

- Le choix du mot de passe.
- Le détournement de compte.
- Virus et chevaux de trois.

- Les cassettes audionumériques (DAT) : les cassettes DAT inventée par Sony, est un support réenregistrable. Le problème est qu'une cassette DAT tient sans difficultés dans une proche de vêtement.
- Entrée frauduleuse via l'Internet.
- L'analyse du trafic.
- Le vol physique.
- La rémanence des données : lorsqu'on crée de l'information, on laisse souvent des traces. Les rubans d'imprimantes, le papier carbone et les feuilles de bourrage jetées à la poubelle peuvent contenir des informations sensibles.

  L'exemple le plus frappant et le plus original est TEMPEST qui est difficile à combattre; les circuits de l'ordinateurs émettent des fréquences de communication radios, ces émanations permettent à un espion disposant de l'équipement adéquat de lire par dessus votre épaule ce qui s'inscrit sur l'écrans de l'ordinateur, la solution, c'est une salle blindé.

Même en répondant à toutes ces questions on n'aura pas un plan d'action parfait, c'est pourquoi, il va falloir les combiner et les compléter avec la méthode décrite dans le graphe suivant :


Analyse et définition
Planification
Implémentation
Maintenance
Définition des besoins de l'entreprise
Evaluation des risques
Conception de l'architecture de sécurité
Develop politiques, procédures
Planification solutions techniques
Sensibilisation des utilisateurs
Sécurité de la connexion Internet
Sécurisation des services professionnels
Sécurisation des services individuels
Gestion, maintenance, audit

# CONCLUSION

A travers ce travail, nous avons pu passer en revue tous les services fournis par Internet et leur utilisation ainsi que les apports pour ceux qui les utilisent. Les utilisations d'Internet par les entreprises sont très variées. Par ses mécanismes techniques et commerciaux, Internet modifie l'échiquier mondial de la transmission de données.

Les opportunités pour les entreprises sont nombreuses, tant en termes d'économies qu'en termes de gains de parts de marché. Elles découvrent régulièrement de nouvelles utilisations du réseau centrées sur leur métier et sur leurs besoins. De nouveaux métiers, de nouveaux secteurs d'activités vont naître du "réseau des réseaux". La prochaine décennie s'annonce riche de changements.

## ***Mise en place d'Internet***

Concernant, la mise en œuvre d'Internet, dans toute la littérature existante la plupart des livres font allusion à l'ensemble des services qu'offre Internet. Mais, quand on pose la question comment faire ? , la réponse en générale est, il faut une connexion auprès d'un fournisseur d'accès, certes c'est une réponse mais elle est incomplète. Certains écris, nous ont permis d'étudier une méthode qu'ils conseillent aux entreprises qui veulent mettre en place Internet. Cette méthode est bonne mais elle est loin d'être complète et parfaite pour éviter tous les pièges que l'entreprise.

Cette méthode définie en quatre étapes la mise en place d'Internet, en commençant par une réflexion sur les besoins et l'information en interne des concernés, puis choix de la connexion et du provider, et finir par la formation. A première vue, cette méthode, insiste sur les différents types connexions possibles avec une analyse des coûts qui s'y rattache. Mais, elle ne détaille pas assez les étapes d'information et de formation des personnes concernées pour que l'entreprise puisse savoir comment s'y prendre. Le point faible de cette méthode est, quelle n'insiste pas assez sur le point du plan de sécurité qui est le point le plus important pour une entreprise car en s'ouvrant sur Internet, elle risque que ses données et ses secrets subissent des attaques de la part de n'importe qui.

Pour revenir sur le point de la connexion, on peut s'apercevoir que si l'on trouve aujourd'hui des solutions de connexion pour un poste isolé à environ 6000 Frs par an, voire beaucoup moins, il faudra compter 90 000 à 120 000 Frs par an pour la liaison d'un réseau local de façon d'un réseau local de façon professionnelle. A l'entreprise de faire en sorte que ce coût soit contrebalancé par une meilleure productivité interne et par gains de communication avec l'extérieur accrus (fournisseurs, filiales, client, prospects). La méthode étudiée donne le même résultat, mais, l'entreprise à besoin de plus que cela car elle veut savoir comment ça marche et le plus important c'est comment décider.

L'un des autres défaut de la méthode est qu'elle met l'accent sur l'entreprise, c'est-à-dire qu'elle ne définit pas assez les relations et les interactions entre le projet, les partenaires et l'entreprise. Ce manque de définition jette un flou sur le déroulement de la méthode.

Ce flou ouvre une optique de recherche sur une méthode complète sur la réalisation d'une méthode claire et complète avec instance sur le mot complète sans oublier qu'elle devra être facile à appliquer.

## ***Mise en place d'Intranet***

Pour la mise en place d'Intranet, la majorité nous fournis la plupart du temps soit les grandes lignes à suivre soit un ensemble de question aux quelles il faut y répondre pour une bonne implémentation. Mais, heureusement, que quelques-uns nous offres d'avantage, telle que Denis LAFONT, qui fournit dans sont ouvrage une méthode détailler et très complète mais très claire au niveau de la terminologie.

Le point fort de cette méthode et quelle met l'accent sur la participation de l'ensemble des différents partenaires interne et externe de l'entreprise vu leur implication majeur dans le fonctionnement de celle-ci.

La voie de recherche ouverte dans ce domaine, touche juste l'amélioration de cette méthode en la complétant par une partie qui permettra de suivre le SI dans son évolution. Donc, une partie qui permettra de faire du prévisionnel.

## ***Mise en place d'un site Web***

Pour la mise en place d'un site web, la littérature est très confuse et insiste trop sur le côté technologie et aucune ne développe le point de la méthodologie ce qui laisse libre cours aux différents utilisateurs que ce soit pour les entreprises ou pour les personnes.

En parcourant, les sites web et les différents ouvrages sur Internet on peut en dégager et en donner une schématisation décrite dans une partie de ce document. Cette partie ouvre la porte à une recherche mais que dans le cadre d'un projet de DEA et ne nécessite pas toute une recherche car la matière première existent et il suffit juste de lui donner un cadre formel et méthodologique.

## ***Mise en place de la sécurité***

En ce qui concerne la mise en ouvre de la sécurité, les ouvrages parlant de sécurité aborde le problème de différentes manières en proposant des méthodes pour la réalisation des solutions. Toutes les méthodes proposées mettent l'accent sur les besoins de l'entreprise en terme de sécurités mais, elles ne leurs disent pas comment s'y prendre. La solution miracle n'existe pas et il faut demander de l'aide extérieure.

Les méthodes proposées sont sous formes soit de questions successives soit de schéma d'étapes. Certes, ces méthodes ont le même objectif mais elles sont très complémentaires. Ce qui induit qu'il faut créer et générer une nouvelle méthode plus complète pour répondre le mieux possible aux attentes des entreprises car tout le monde connais l'importance de la sécurité pour celle-ci.

On peut dire aussi que tant qu'une loi sur le cryptage des informations n'est pas reconnue au niveau international, la sécurité des messages en transitant sur les réseaux locaux et Internet ne sera pas assurée de façons catégorique car la sécurité 100% n'existe pas.

# RÉFÉRENCES BIBLIOGRAPHIQUES

🗁 Notes de cours (du DESS-RADI, Université de CAEN et de Anne BEGIN du CNET de CAEN ).

## Articles

🕮 Jean-Luc ARCHIMBAUD, "L'Internet Professionnel : Présentation de l'Internet", CNRS Editions, Février1995, p. 15-64.

🕮 Jean-Luc ARCHIMBAUD, "L'Internet Professionnel : Présentation Technique des Services", CNRS Editions, Février1995, p. 65-124.

🕮 Marion BOUGERAD, "Deux PME sur Trois ouvriront un site web avant l'an 2000", Magazine l'Internet Professionnel, n°20, Mai 1998, p. 8-9.

🕮 Denis LAFONT, "L'Internet Professionnel : l'Internet vu par l'entreprise", CNRS Editions, Février1995, p. 313- 315.

## Ouvrages

🕮 Alain BENSOUSSAN, "Internet aspects juridiques", Editions HERMES , 1996, 128 pages.

🕮 Richard J. SMITH & Mark GIBBS, "Internet", Editions SYBEX, Collection LVRE D'OR, 1996, 763 pages.

🕮 John R. LEVINE & Carol BAROUDI, "Internet : les fondamentaux", Edition THOMSON Publishing, 1996, 976 pages.

🕮 Oliver ANDRIEU & Denis LAFONT, "Internet et l'Entreprise", Editions EYROLLES, 1995, 395 pages.

🕮 Magazine l'Internet Professionnel, "Le Guide du Web Master", First Editions, 1997, 482 pages.

🕮 Chapitre "Commerce électronique" du Livre Blanc de l'AFTEL (Association Française de la Télématique), "Internet : les enjeux pour la France", Edition AFTEL, 1997.

🕮 Alain MASSER, "Internet, la révolution est pour demain", les Editions du Téléphone, 1996, 335 pages.

🕮 Frédérique ALIN & Denis LAFONT & Jean - François MACARY, "Le Projet Intranet", Editions EYROLLES, novembre 1996, 257 pages.

📖 Andrew THANENBAUM, " Réseaux ", Éditions InterEditions (PARIS) et Éditions PRENTICE HALL (LONDRE), 1997, 792 pages.

📖 Michel GERMAIN, "L'Intranet", Editions ECONOMICA Collection Gestion Poche, 1998, 112 pages.

## Rapport

📖 Francis LORENTZ," Commerce électronique : une nouvelle donne pour les consommateurs, les entreprises, les citoyens et les pouvoirs publics ", Rapport de Groupe de Travail, Ministère de l'Économie, des Finances et de l'Industrie, 7 janvier 1998, "http://www.finances.gouv.fr/commerce_electronique/lorentz/sommaire.html".

## LOIS

📖 "La réglementation française en matière de cryptologie" ,Service Central de la Sécurité des Systèmes d'Information et Secrétariat d'Etat à l'Industrie et Service des Industries de Communication et de Service, Juin 1998, "http://www.telecom.gouv.fr/francais/telecharg/cryp_w97.doc".

## Sites Web

💻 Site de l'Unité Réseaux (UREC) du CNRS "http://www.urec.fr".

💻 Site de l'UNIG "http://www.imaginet.fr/ime".

💻 Site du chapitre français de l'ISOC "http://www.isoc.asso.fr".

💻 Site de l'AFTEL "http://www.aftel.fr".

💻 Site du Ministère de l'Économie et des Finances "http://www.finances.gouv.fr".

💻 Site du Ministère de l'industrie sur les télécommunications, les technologies et services de l'information, le secteur postal "http://www.telecom.gouv.fr/francais.htm".

# GLOSSAIRE

- **Archie :** est un logiciel de bases de données permettant de localiser un fichier Internet afin de la récupérer à l'aide de FTP.
- **Bande Passante :** c'est la quantité d'information que peut véhiculer un canal de communication et elle se mesure en bits par seconde (*bps*).
- **CGI :** (*Common Gateway Interface*) ce sont des programmes qui sont lancés et exécutés sur le serveur HTTP après envoi par la lecture d'un formulaire.
- **Chiffrement :** (*Cipher*) consiste à brouiller l'information de sorte qu 'elle ne puisse être lue que par les personnes autorisées.
- **Clé privée :** (*Private Key*) une des deux clés est nécessaire pour un système clé publique ou asymétrique. La clé privée est habituellement gardée secrète par propriétaire.
- **Clé publique :** (*Public Key*) une des deux clés est nécessaire dans une cryptographie à clé publique ou asymétrique. La clé publique est habituellement annoncée au reste du monde.
- **Client :** C'est un programme qui est utilisé pour contacter un serveur. On parle alors de modèle client/serveur. L'avantage du modèle est que le client sait faire un certain nombre de tâches et ne soumet au serveur que les informations nécessaires. D'autre part un serveur peut fournir des clients sur PC Macintosh ou machine Unix.
- **Client/Serveur :** est un modèle dont la communication prend généralement d'un message client demandant au serveur de réaliser telle ou telle tâche. Le serveur fait alors le travail demandé et renvoie une réponse. Dans la plupart des cas, il y a un grand nombre de clients qui s'adressent à un petit nombre de serveurs.
- **Connexion :** installation permettant de relier un ordinateur et le réseau Internet.
- **Dial-up IP :** se dit des connexions au réseau Internet par composition d'un numéro de téléphone. Ce terme désigne des connexions temporaires, par opposition aux connexions permanentes sur les lignes louées.
- **DNS :** (*Domaine Name Server*) c'est un serveur qui à partir d'une adresse de la forme nom.domaine.organisation sait indiquer l'adresse IP qui est la seule comprise par les ordinateurs.
- **E-Mail ou Mail :** C'est le courrier électronique. Le terme français académique se voudrait être émel.
- **Firewall :** c'est un ordinateur que l'on met entre un réseau local comme celui de l'entreprise et un autre réseau qui peut être Internet. Il fait office de filtre afin d'assurer la sécurité des informations à l'intérieur du réseau local.
- **Formulaire :** il comporte des boîtes ou/et des boutons qui permettent à l'utilisateur de remplir un questionnaire ou de faire certains choix ou d'envoyer le tout au propriétaire du (ou des) formulaire(s).
- **Freeware :** c'est un logiciel que son auteur a choisi de rendre absolument gratuit, soit qu'il désire le tester, soit qu'il désire en faire profiter la communauté.
- **FTP :** (*File Transfert Protocol*) protocole d'échange de fichiers entre sites informatiques. En général les sites ouverts au public sont dits *anonymous FTP* car le nom de *login* est *anonymous*.
- **FTP anonymous :** service FTP sur lequel l'utilisateur peut se connecter sans posséder un compte utilisateur, mais avec le nom *anonymous*. Il est demandé de renseigner le mot de passe avec son adresse courrier.
- **GIF :** (*Graphic Interchange Format*) est un format de fichier créé sur CompuServe pour

compresser le images sans perdre pour autant leur qualité. Devenu standard, il est utilisé dans plusieurs réseaux.

- **Gopher :** est un modèle Client/Serveur permettant de lire des menus distants sur une machine.
- **HTML :** (*HyperText Markup Langage*) les pages web sont écrites dans un format assez simple, appelé html. On peut voir le contenu d'une page html dans un des menus du lecteur de web en demandant à voir le code source de la page.
- **HTTP :** (*HyperText Tranfert Protocol*) un serveur http est chargé d'envoyer les pages web (en HTML) à votre ordinateur, lorsque vous lisez une page web.
- **IMAP :** (*Interactive Mail Access Protocol*) a été conçu pour satisfaire l'utilisateur qui dispose de plusieurs ordinateurs comme par exemple une station au bureau et un PC à la maison et un portable entre les deux. Imap ne copie pas le courrier sur l'ordinateur de l'utilisateur puisqu'il en plusieurs.
- **Internet :** est le réseau des réseaux qui rassemble des centaines de millions d'utilisateurs. Le réseau est constitué de plusieurs millions de machines à travers le monde et offre des services très divers (diffusion d'information, forums de discussion thématiques,….).
- **Intranet :** constitue un mini Internet privé (sur réseau local) limité à une entreprise pour rendre des services internes divers (diffusion d'information, publicité de certaine activités,….) et c'est une réplication des protocoles utilisés sur Internet à l'intérieur de l'entreprise.
- **ISOC :** (*Internet Society*) la société d'Internet est formée de volontaires qui offrent gratuitement leur temps pour faire valoir et promouvoir les objectifs d'Internet. Elle est dirigée par l'IAB (*Internet Archtecture Board*) et qui ratifie les standards fournis et mis au point par les membres de l'ISOC.
- **JAVA :** langage mis au point par la société SUN s'exécutant sur toutes les plates-formes matérielles et qui peut être utilisé sous forme d'applet qui interprétés dans les navigateurs.
- **JavaScript :** langage permettant de contrôler le navigateur et le langage HTML avec les richesses fonctionnelles que ne permet pas HTML.
- **JPEG :** (*Joint Photographic Experts Groups*) permet la compression d'images fixes de qualité photo. Elle a été définie par un groupe mixte au sens où ses experts provenaient de l'UIT, de l'ISO et de la CEI.
- **MIME :** (*MultiPurpose Internet Mail Extensions*) système d'encodage permettant d'expédier des fichiers attachés au courrier électronique.
- **Modem :** (*modulateur/démodulateur*) boîtier que l'on met entre l'ordinateur et une prise téléphonique pour transformer un signal numérique (informatique) en signal analogique téléphonique et vise versa.
- **Navigateur :** il charge les pages Web demandées, interprète le texte de formatage qu'il contient et affiche à l'écran la page correctement formatée.
- **News :** les news sont des forums où chacun dépose des courriers (articles) par thème. Ces courriers sont conservés quelques jours et donnent lieu à des discussions.
- **Newsgroup :** ou les groupes d'intérêt sont des forums spécialisés dans lesquels les utilisateurs peuvent échanger des informations. Chaque groupe a sont style, ses usages et son étiquette, qu'il convient de respecter scrupuleusement.
- **NFS :** (*Network File System*) système permettant de donner accès aux fichiers d'un ordinateur éloigné comme s'il s'agissait d'un disque local.
- **NNTP :** (*Network News Tranfer Protocol*) est un protocole de transfert de nouvelles, il a deux objectifs, permettre l'envoi de nouveaux articles sur des liaisons fiables et permettre aussi aux utilisateurs qui n'ont que des micro-ordinateurs de lire correctement les nouvelles à distance.

- **Ordinateur Hôte :** () est un ordinateur situé au centre d'un réseau ou un sous-réseau qui exécute les programme des utilisateurs donc des applications et la communication entre réseaux se fait toujours entre les hôtes. Ce terme est très largement utiliser pour designer un ordinateur directement relié à Internet.
- **Passerelle :** (*Gateways*) est souvent utiliser pour interconnecter des réseaux différents et parfois incompatibles que ce soit des LAN ou des WAN. Elle fait aussi les traductions nécessaires, à la fois en termes de matériel et de logiciel.
- **PGP :** (*Pretty Good Privacy*) logiciel d'encodage de données pour le Mail, afin d'assurer la confidentialité des messages.
- **POP :** (*Post Office Protocol*) protocole permettant à utilisateur connecté sur une ligne intermittente d'interroger son courrier situé dans la boîte aux lettres de son serveur ou fournisseur.
- **PPP :** (*Poin to Point Protocol*) protocole permettant d'utiliser une ligne téléphonique et un modem en TCP/IP. Remplace peu à peu le protocole SLIP.
- **Protocole :** le mot protocole désigne en général les messages échangés entre deux machines. L'intérêt d'un protocole est de définir des méthodes d'échange d'information, indépendantes des matériels. Ainsi, une fois le protocole défini, chaque terminal, ou client ou serveur implémente ce protocole sans se soucier des autres ordinateurs.
- **Provider :** est le nom anglais donné au fournisseur d'accès Internet que ce soit une entreprise ou un organisme ou autres.
- **Requête :** Ordre (adressé au SGBD) de restituer un ensemble précis de données. Appelée aussi extraction.
- **RFC :** (*Request For Comments*) succession d'articles classés au sujet d'Internet. Ce sont les RFC qui explicitent les normes Internet.
- **Réseau :** est un ensemble d'ordinateurs séparés mais interconnectés qui exécutent des tâches différentes.
- **RTC :** (*Réseau Téléphonique Commuté*) est le système de communication du réseau téléphonique qui permet de relier les modems des PC ou des portable aux réseaux Internet.
- **Serveur :** un ordinateur qui fournit des services à des clients. Il fournit ces services à des ordinateurs par des messages ce qui permet d'avoir plusieurs type de clients.
- **Shareware :** c'est un logiciel que chacun peut essayer pendant une durée de temps définie après la quelle on doit acquitter des droits.
- **SMTP :** (*Simple Mail Transfert Protocol*) protocole de gestion des courriers électriques sur Internet.
- **TCP/IP :** est le nom de la partie cachée de l'Internet. Il existe plusieurs protocoles réseau (Netware, LanManager...). TCP/IP est le plus propice aux interconnexions de réseaux. L'Internet Protocol (IP) est un protocole en mode connecté permettant l'adressage et le routage des datagrammes. TPC (*Transmission Control Protocol*) est un protocole en mode connecté permettant le transfert fiable en bout des données applicatives.
- **Telnet :** logiciel permettant de se connecter sur un serveur pour y exécuter des commandes.
- **Terminal :** (ou émulateur de terminal) est un programme permettant à un ordinateur de communiquer avec un ordinateur hôte distant comme s'il s'agissait d'un type spécifique de terminal directement relié à cet ordinateur ou au réseau.
- **UNIX :** système d'exploitation libre d'accès utilisé pour faire fonctionner les serveurs.
- **WAIS :** (*Wide Area Information Servers*) système de base de données textuelle qui est utilisé pour l'indexation des mots importants dans les pages web.
- **WebMaster :** est la personne responsable d'un site web.
- **Windows :** système d'exploitation de Microsoft utilisé pour faire fonctionner les micro-

odinateurs et les serveurs.

- **WWW :** (*World Wide Web*) système mondial d'interconnexion des informations par le protocole web.
- **X-windows :** est un système de fenêtrage répandu, s'appuyant sur le réseau, qui permet à beaucoup de programmes de partager un seul affichage graphique. Les programmes X-windows présentent leurs écrans dans des fenêtres qui peuvent être soit sur l'ordinateur sur lequel s'exécute le programme, soit sur tout autre ordinateur qui est sur le réseau.
- **X500 :** Norme de l'Organisation de standardisation internationale (ISO) définissant l'annuaire universel.