Université Mouloud MAMMERI de Tizi-Ouzou
Faculté de Génie Electrique et d'Informatique
Département d'Informatique

Mémoire de Fin d'études
En vue de l'obtention du diplôme de Master en Informatique
Spécialité : Conduite de Projets Informatiques(CPI)

Thème :

Sécurité des Systèmes d'Information (SSI)

Encadré par : Mr M.OUAMRANE
Réalisé par : Mr DAHMANE Mourad

Juin 2014

Remerciements

D’abord je tiens à exprimer mes plus vifs remerciements à mon promoteur Mr M.OUAMRANE pour sa disponibilité, les nombreux conseils, orientations et encouragements qu'il a su me prodiguer durant mon travail.

Aussi je tiens à lui reconnaître le temps précieux qu’il m’a consacré.

Je voudrais également exprimer mes sincères remerciements aux membres du jury qui m’ont fait l’honneur d’accepter de juger mon travail.

Merci à tous qui ont contribué de prés ou de loin, à la réalisation de ce travail.

Table des figures

Les systèmes d'information prennent de plus en plus une place stratégique au sein des entreprises. Ainsi la notion du risque lié à ces derniers devient une source d'inquiétude et une donnée importante à prendre en compte, ceci en partant de la phase de conception d'un système d'information jusqu'à son implémentation et le suivi de son fonctionnement.

Les pratiques associées à la sécurité des systèmes d'information constituent un point à l'importance croissante dans l'écosystème informatique qui devient ouvert et accessible par utilisateurs, partenaires et fournisseurs de services de l'entreprise. Il devient essentiel pour les entreprises de connaître leurs ressources en matière de système d'information et de définir les périmètres sensibles à protéger afin de garantir une exploitation maîtrisée et raisonnée de ces ressources.

Par ailleurs, les nouvelles tendances de nomadisme et de l'informatique « in the Cloud » permettent, non seulement, aux utilisateurs d'avoir accès aux ressources mais aussi de transporter une partie du système d'information en dehors de l'infrastructure sécurisée de l'entreprise. D'où la nécessité de mettre en place des démarches et des mesures pour évaluer les risques et définir les objectifs de sécurité à atteindre.

Ainsi la sécurité informatique est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires pour conserver, rétablir et garantir la sécurité du système d'information.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi.

La sécurité est aujourd'hui un des enjeux considérables des systèmes, que se soit vis-à-vis de la productivité, des montants financiers, de l'image de marque ou des aspects légaux. Avec la mise en ligne des systèmes et l'augmentation du nombre d'utilisateurs, et donc d'attaquants potentiels y compris internes,

Le piratage repose essentiellement sur les erreurs de conception des systèmes et sur des mauvais paramétrages lors des configurations de ces derniers, ainsi que sur des failles de sécurité présentes dans les différents services proposés. Nous assistons alors à la mise en place d'une compétition entre les pirates et les personnes en charge de la sécurisation des systèmes tels que les administrateurs réseaux ou les personnes en charge du développement des logiciels. Les premiers cherchent à exploiter par tous les moyens les trous de sécurité présents. Les seconds tentent de sécuriser le système d'information. La conséquence est que la sécurité est devenue un véritable enjeu pour les entreprises qui veulent protéger leur système d'information et leurs sites de commerce électronique

L'efficacité de la sécurité d'un système d'information ne repose pas uniquement sur les outils de sécurité mais également sur une stratégie, une organisation et des procédures cohérentes. Cela nécessite une structure de gestion adéquate dont la mission est de gérer, mettre en place, valider, contrôler et faire comprendre à l'ensemble des acteurs de l'entreprise l'importance de la sécurité. Elle détermine également le comportement, les privilèges, les responsabilités de chacun. Elle spécifie, en fonction de facteurs critiques de succès qui permettent d'atteindre les objectifs de l'entreprise, les mesures et directives sécuritaires appropriées. Ces dernières doivent être cohérentes par rapport aux plans d'entreprise et informatique. Pour cela, une vision stratégique de la sécurité globale de l'entreprise est nécessaire.

Les systèmes d'information (SI) deviennent de plus en plus complexes. Ces systèmes combinent souvent des infrastructures de réseau fixes et mobiles (sans fil), reposant sur divers systèmes d'exploitation (Windows, Linux, Unix, MacOS, etc) et fournissent de nombreuses applications (messageries, navigateurs, serveurs de bases de données, services web, etc).
Dans ce contexte, définir et ensuite gérer une politique de sécurité est une tâche complexe pour les Administrateurs.

On peut déduire de ces constats que la démarche de sécurité informatique est une activité managériale des systèmes d'information et qu'il convient aussi d'établir un tableau de bord de pilotage associé à une politique de sécurité comprenant les organes vitaux constituant une entreprise.

Dans ce mémoire nous allons, dans un premier temps, présenter d'une façon générale les différents aspects liés à la sécurité informatique. Nous verrons ensuite dans le deuxième chapitre les types d'attaques informatiques et les techniques d'attaques à disposition des pirates. Nous étudierons dans le troisième chapitre Les principaux dispositifs techniques permettant de sécuriser un système d'information et dans le dernier chapitre nous verrons comment mettre en place une politique de sécurité sous l'angle organisationnel.

Une conclusion générale viendra clore ce travail résumant les grands points qui ont été abordés dans ce mémoire.

Chapitre I : Généralités sur la sécurité des systèmes d'information(SSI)

I.1. Introduction :

La sécurité est un enjeu majeur des technologies numériques modernes. Infrastructures de télécommunication (GSM, GPRS, UMTS), réseaux sans fils (Bluetooth, Wi-Fi, WiMax), Internet, systèmes d'information, routeurs, ordinateurs, téléphones, décodeurs de télévision, assistants numériques, systèmes d'exploitation, applications informatiques, toutes ces entités présentent des vulnérabilités : faille de sécurité, défaut de conception ou de configuration. Ces systèmes tombent en panne, subissent des erreurs d'utilisation et sont attaqués de l'extérieur ou de l'intérieur par des pirates ludiques, des cybercriminels, ou sont la proie d'espionnage industriel.

Une approche globale de la sécurité des systèmes est essentielle pour protéger la vie privée, pour défendre le patrimoine d'une entreprise ou pour réduire les vulnérabilités des grands systèmes d'information.

Ce chapitre présente d'abord les différents aspects de la sécurité : propriétés et enjeux de sécurité, menaces, risques et vulnérabilités et puis donne une idée générale sur les méthodes d'attaques, mécanismes et services de sécurité.

I.2. Définitions :

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques. Elle est intrinsèquement liée à la sécurité de l'information et des systèmes d'information. [1]

La sécurité informatique est un processus perpétuel visant à améliorer le niveau de sécurité en instaurant une politique de sécurité au sein des organismes et en palliant à certaines faiblesses à la fois organisationnelles et technologiques.

La **sécurité des systèmes d'information** (**SSI**) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information.

La sécurité du Système d'Information est un processus qui contribue à la qualité et assure la protection des personnes, du patrimoine informationnel et des matériels contre les menaces externes et internes. Cet objectif de sécurité repose sur des solutions techniques adaptées, et se construit autour d'une organisation régie par une politique de sécurité en conformité avec les lois en vigueur et les exigences de l'entreprise.

Les normes pour la sécurité de l'information, permettent la définition d'un véritable processus qualité pour la sécurité de l'information. Des moyens humains, des solutions et des procédures seront nécessaires pour le définir, le mettre en œuvre, en assurer le support et le changement, et le contrôler en vue de son amélioration.

La Sécurité des systèmes d'information (SSI) est un domaine extrêmement vaste puisqu'elle fait appel à de nombreux concepts juridiques, sociaux, et économiques, à la gestion de personnel, et à des connaissances techniques extrêmement pointues.

Il existe plusieurs technologies et problématiques de sécurité :

- les réseaux informatiques peuvent reposer sur un grand nombre de technologies de réseaux de transport (Wi-Fi, IPv4, IPv6, MPLS, ATM) ;
- ces technologies évoluent pour permettre une plus grande mobilité aux utilisateurs et le support d'une plus large palette de services (messagerie, services de transactions électroniques, téléphonie sur IP, cloud computing, RFID) ;
- les technologies reposent sur des services réseaux critiques (annuaires LDAP, DNS, routage de trafic) mettant en jeu des terminaux, mais aussi des équipements de réseaux (routeurs, commutateurs) ;
- les acteurs de la SSI sont très variés (opérateurs, fournisseurs de services, administrateurs de réseaux privés, simples particuliers, constructeurs d'équipements, éditeurs logiciels).

I.3. Enjeux de la sécurité informatique:

Plusieurs types d'enjeux doivent être maitrisés :

***1. L'intégrité* :** Les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire.

***2. La confidentialité* :** Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

***3. La disponibilité* :** Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

***4. La non-répudiation et l'imputation* :** Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

***5. L'authentification* :** L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

La sécurité informatique est un défi d'ensemble qui concerne une chaine d'éléments : Les infrastructures matérielles de traitement ou de communication, les logiciels (systèmes d'exploitation ou applicatifs), les données, le comportement des utilisateurs. Le niveau global de sécurité étant défini par le niveau de sécurité du maillon le plus faible, les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

I.4. Critères de sécurité :

La sécurité peut s'évaluer suivant plusieurs critères :

- **Disponibilité :** garantie que ces éléments considérés sont accessibles au moment voulu par les personnes autorisées.
- **Intégrité :** garantie que les éléments considérés sont exacts et complets.
- **Confidentialité :** garantie que seules les personnes autorisées ont accès aux éléments considérés. [1]

D'autres aspects peuvent éventuellement être considérés comme des critères (bien qu'il s'agisse en fait de fonctions de sécurité), tels que :

- **Traçabilité** (« **Preuve** » ou « auditabilité »)**:** garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

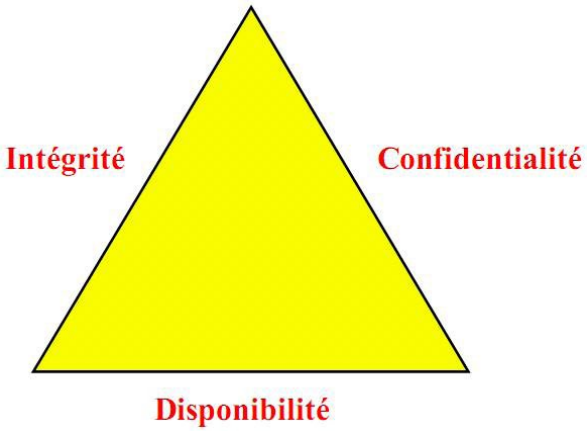


Figure 1 : Les propriétés de sécurité informatique

I.5. Présentation de l'insécurité informatique :

I.5.1. Les menaces :

La menace est l'éventualité alarmante que quelque chose se produise, et qui pourra porter atteinte à un système informatique, en d'autres termes, une menace est un événement ou action susceptible de violer la sécurité d'un système informatique. La menace informatique représente le type d'actions susceptibles de nuire dans l'absolu à un système informatique [2]. En termes de sécurité informatique les menaces peuvent être le résultat de diverses actions en provenance de plusieurs origines :

- **Origine opérationnel:**

  Ces menaces sont liées à un état du système à un moment donné. Elles peuvent être le résultat d'un bogue logiciel (Buffer Overflows, format string …etc.), d'une erreur de filtrage des entrées utilisateur (typiquement les XSS et SQL injection), d'un dysfonctionnement de la logique de traitement ou d'une erreur de configuration

- **Origine physique:**

  Elles peuvent être d'origine accidentelle, naturelle ou criminelle. On peut citer notamment les désastres naturels, les pannes ou casses matérielles, le feu ou les coupures électriques.

- **Origine humaine:**

  Ces menaces sont associées directement aux erreurs humaines, que ce soit au niveau de la conception d'un système d'information ou au niveau de la manière dont on l'utilise. Ainsi elles peuvent être le résultat d'une erreur de conception ou de configuration comme d'un manque de sensibilisation des utilisateurs face au risque lié à l'usage d'un système informatique.

Les principales menaces auxquelles un système d'information peut être confronté sont :

- un **utilisateur du système** : l'énorme majorité des problèmes liés à la sécurité d'un système d'information a pour origine un utilisateur, généralement insouciant. Il n'a pas le désir de porter atteinte à l'intégrité du système sur lequel il travaille, mais son comportement favorise le danger ;
- une **personne malveillante** : une personne parvient à s'introduire sur le système, légitimement ou non, et à accéder ensuite à des données ou à des programmes auxquels elle n'est pas censée avoir accès. Le cas fréquent est de passer par des logiciels utilisés au sein du système, mais mal sécurisés;
- un **programme malveillant** : un logiciel destiné à nuire ou à abuser des ressources du système est installé (par mégarde ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données ; des données confidentielles peuvent être collectées à l'insu de l'utilisateur et être réutilisées à des fins malveillantes ;
- un **sinistre** (vol, incendie, dégât des eaux) : une mauvaise manipulation ou une malveillance entraînant une perte de matériel et/ou de données.

I.5.2. Vulnérabilité :

Dans le domaine de la sécurité informatique, une **vulnérabilité** ou **faille** est une faiblesse dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient. [2]

Ces vulnérabilités sont la conséquence de faiblesses dans la conception, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système, mais il s'agit généralement de l'exploitation de bugs logiciels. Ces dysfonctionnements logiciels sont en général corrigés à mesure de leurs découvertes, c'est pourquoi il est important de maintenir les logiciels à jour avec les correctifs fournis par les éditeurs de logiciels.

Il arrive que la procédure d'exploitation d'une faille d'un logiciel soit publiquement documentée et utilisable sous la forme d'un petit logiciel appelé « exploit ».

- **Exemples de vulnérabilités :**

Les vulnérabilités ci-dessous font partie des plus connues :

- dépassement de tampon ;
- injection SQL ;
- cross site scripting.

➢ **Pourquoi les systèmes sont vulnérables ?**

- La sécurité est chère et difficile et il y a un manque de budget pour ça mise en œuvre dans quelques entreprises.
- -La sécurité ne peut être sûre à 100%, elle est même souvent inefficace.
- Les organisations acceptent de courir le risque, la sécurité n'est pas une priorité.
- De nouvelles technologies (et donc vulnérabilités) émergent en permanence.
- Les systèmes de sécurité sont faits, gérés et configurés par des hommes.
- Il n'existe pas d'infrastructure pour les clefs et autres éléments de cryptographie

➢ **Publication d'une vulnérabilité :**

***Méthode de publication* :**

La méthode de publication des vulnérabilités est un sujet qui fait débat au sein de la communauté de la sécurité des systèmes d'information. Certains affirment qu'il est nécessaire de publier immédiatement toutes les informations à propos d'une vulnérabilité dès qu'elle a été découverte *(full disclosure)*. D'autres prétendent qu'il est préférable de limiter en premier lieu la publication uniquement aux utilisateurs qui en ont un besoin important (divulgation responsable, voire coordonnée), puis après un certain délai, de publier en détail, s'il y a besoin.

Ces délais peuvent permettre de laisser le temps aux développeurs de corriger la vulnérabilité et à ces utilisateurs d'appliquer les patchs de sécurité nécessaires, mais peuvent aussi accroître les risques pour ceux qui n'ont pas ces informations [2]. Les éditeurs de logiciels appellent cette méthode de publication la « divulgation responsable » et encouragent les chercheurs en sécurité à l'utiliser [1]. En théorie, ces délais permettent aux éditeurs de publier les correctifs nécessaires pour protéger leurs logiciels et leurs utilisateurs, mais en pratique, cela ne les contraint pas à corriger les vulnérabilités. Il a ainsi pu arriver que certaines vulnérabilités soient restées non corrigées pendant des mois voire des années, tant qu'aucun exploit n'a été publié. Devant cette situation, certains ont décidé de laisser un délai - considéré raisonnable - aux éditeurs pour corriger les vulnérabilités avant de les divulguer.

I.5.3. Les risques :

Le risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système. Traiter le risque c'est prendre en compte les menaces et les vulnérabilités. Il est important de mesurer les risques, non seulement en fonction de la probabilité ou de la fréquence de leurs survenances, mais aussi en mesurant leurs effets possibles. [2]
Ces effets, selon les circonstances et le moment où ils se manifestent, peuvent avoir des conséquences négligeables ou catastrophiques.

- ✓ Données irrémédiablement perdues ou altérées, ce qui les rend inexploitables.
- ✓ Données ou traitements durablement indisponibles, pouvant entraîner l'arrêt d'une production ou d'un service.

- ✓ Divulgation d'informations confidentielles ou erronées pouvant profiter à des sociétés concurrentes ou nuire à l'image de l'entreprise.
- ✓ Déclenchement d'actions pouvant provoquer des accidents physiques ou induire des drames humains.

➢ **Facteurs du risque :**

Il y'a risque lorsqu'il y'a combinaison de menace et de vulnérabilité, et ces deux composants forment la base du risque. Ainsi, s'il n'y a pas de menace, il n'y a aucun risque, et de même s'il n'y a pas de vulnérabilité, il n'y a aucun risque [2].

➢ **Niveaux des risques :**

Le risque peut être qualitativement défini selon trois niveaux :

- ✓ **Mineur :** La vulnérabilité expose l'entreprise à un risque, mais il est improbable que « quoi que ce soit » puisse se produire. Il faut si possible, prendre des mesures pour supprimer cette vulnérabilité, mais il ne faut pas que le coût de cette action soit trop important par rapport à une réduction minime du risque.
- ✓ **Moyen :** La vulnérabilité présente un risque important pour la confidentialité, l'intégrité, la disponibilité des informations de l'entreprise, des systèmes ou des sites physiques. Il y a une réelle possibilité que cela puisse arriver. Il est recommandé de supprimer cette vulnérabilité.
- ✓ **Majeur :** La vulnérabilité présente un danger réel pour la confidentialité, l'intégrité et la disponibilité « des informations, des systèmes ou des sites physiques ». Il faut prendre des mesures immédiates pour supprimer cette vulnérabilité. [A3]

I.5.3.1. Risques humains :

Les risques humains sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés. Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

- ✓ ***La maladresse* :** comme en toute activité, les humains commettent des erreurs ; il leur arrive donc plus ou moins fréquemment d'exécuter un traitement non souhaité, d'effacer involontairement des données ou des programmes, etc.
- ✓ ***L'inconscience et l'ignorance* :** de nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils encourent aux systèmes qu'ils utilisent, et introduisent souvent des programmes malveillants sans le savoir. Des manipulations inconsidérées (autant avec des logiciels que physiques) sont aussi courantes.
- ✓ ***La malveillance* :** aujourd'hui, il serait quasiment inconcevable de prétexter l'ignorance des risques suscités, tant les médias ont pu parler des différents problèmes de virus et de vers ces dernières années (même s'ils ont tendance, en vulgarisant, à se tromper sur les causes et les problèmes). Ainsi, certains utilisateurs, pour des raisons très diverses, peuvent volontairement mettre en péril le système d'information, en y introduisant en connaissance de cause des virus (en connectant par exemple un ordinateur portable sur un réseau d'entreprise), ou en introduisant volontairement de mauvaises informations dans une base de données [A3]. De même il est relativement aisé pour un informaticien d'ajouter délibérément des fonctions cachées lui permettant, directement ou avec l'aide de complices, de détourner à son profit de l'information ou de l'argent.
- ✓ ***L'ingénierie sociale* :** l'ingénierie sociale (*social engineering* en anglais) est une méthode pour obtenir d'une personne des informations confidentielles, que l'on n'est pas normalement autorisé à obtenir, en vue de les exploiter à d'autres fins (publicitaires par exemple) [1]. Elle consiste à se faire passer pour quelqu'un que l'on n'est pas (en

général un administrateur) et de demander des informations personnelles (nom de connexion, mot de passe, données confidentielles, etc.) en inventant un quelconque prétexte (problème dans le réseau, modification de celui-ci, heure tardive, etc.). Elle peut se faire soit au moyen d'une simple communication téléphonique, soit par courriel, soit en se déplaçant directement sur place.

- ✓ ***L'espionnage*** **:** l'espionnage, notamment industriel, emploie les mêmes moyens, ainsi que bien d'autres (influence), pour obtenir des informations sur des activités concurrentes, procédés de fabrication, projets en cours, futurs produits, politique de prix, clients et prospects, etc. [3]
- ✓ ***Le détournement de mot de passe*** **:** un administrateur système ou réseau peut modifier les mots de passe d'administration lui permettant de prendre le contrôle d'un système ou d'un réseau.

I.5.3.2. Risques techniques :

Les risques techniques sont tout simplement ceux liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels [2]. Ces incidents sont évidemment plus ou moins fréquents selon le soin apporté lors de la fabrication et des tests effectués avant que les ordinateurs et les programmes ne soient mis en service. Cependant les pannes ont parfois des causes indirectes, voire très indirectes, donc difficiles à prévoir.

- ✓ ***Incidents liés au matériel*** **:** si on peut le plus souvent négliger la probabilité d'une erreur d'exécution par un processeur (il y eut néanmoins une exception célèbre avec l'une des toutes premières générations du processeur Pentium d'Intel qui pouvait produire, dans certaines circonstances, des erreurs de calcul), la plupart des composants électroniques, produits en grandes séries, peuvent comporter des défauts et finissent un jour ou l'autre par tomber en panne. Certaines de ces pannes sont assez difficiles à déceler car intermittentes ou rares.
- ✓ ***Incidents liés au logiciel*** **:** ils sont de très loin les plus fréquents ; la complexité croissante des systèmes d'exploitation et des programmes nécessite l'effort conjoint de dizaines, de centaines, voire de milliers de programmeurs. Individuellement ou collectivement, ils font inévitablement des erreurs que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité. Des failles permettant de prendre le contrôle total ou partiel d'un ordinateur sont régulièrement rendues publiques et répertoriées sur des sites comme SecurityFocus ou Secunia [1]. Certains programmes sont conçus pour communiquer avec internet et il n'est donc pas souhaitable de les bloquer complètement par un pare-feu (navigateur web par exemple).
- ✓ ***Incidents liés à l'environnement*** **:** les machines électroniques et les réseaux de communication sont sensibles aux variations de température ou d'humidité (tout particulièrement en cas d'incendie ou d'inondation) ainsi qu'aux champs électriques et magnétiques. Il n'est pas rare que des ordinateurs connaissent des pannes définitives ou intermittentes à cause de conditions climatiques inhabituelles ou par l'influence d'installations électriques notamment industrielles (et parfois celle des ordinateurs eux-mêmes).

Pour s'en prémunir, on recourt généralement à des moyens simples bien que parfois onéreux :

- ✓ ***Redondance des matériels* :** la probabilité ou la fréquence de pannes d'un équipement est représentée par un nombre très faible (compris entre 0 et 1, exprimé sous la forme 10^{-n}). En doublant ou en triplant (ou plus) un équipement, on divise le risque total par la probabilité de pannes simultanées. Le résultat est donc un nombre beaucoup plus faible ; autrement dit l'ensemble est beaucoup plus fiable (ce qui le plus souvent reporte le risque principal ailleurs).[2]
- ✓ ***Dispersion des sites* :** Un accident (incendie, tempête, tremblement de terre, attentat, etc.) a très peu de chance de se produire simultanément en plusieurs endroits distants.
- ✓ ***Programmes ou procédures de contrôle indépendant* :** ils permettent bien souvent de déceler les anomalies avant qu'elles ne produisent des effets dévastateurs.

I.5.3.3. Risques juridiques :

L'ouverture des applications informatiques par le web et la multiplication des messages électroniques augmentent les risques juridiques liés à l'usage des technologies de l'information [1]. On peut citer notamment :

- le non-respect de la législation relative à la signature numérique.
- les risques concernant la protection du patrimoine informationnel.
- le non-respect de la législation relative à la vie privée.
- le non-respect des dispositions légales relatives au droit de la preuve. [A3]

I.5.4. Attaque :

Une attaque est toute action compromettant la sécurité de l'information

C'est la réalisation d'une menace. C'est une atteinte à l'une des composantes de la sécurité :

- ✓ Confidentialité ➔ divulgation des données.
- ✓ Intégrité ➔ Falsification ou modification des données.
- ✓ Disponibilité ➔ dénis de service.

Les attaques sont classées en quatre types génériques [4] :

- ✓ Interruption : Attaque sur la disponibilité.
- ✓ Interception : Attaque sur la confidentialité.
- ✓ Modification : Attaque sur l'intégrité.
- ✓ Fabrication : Attaque sur l'authenticité.

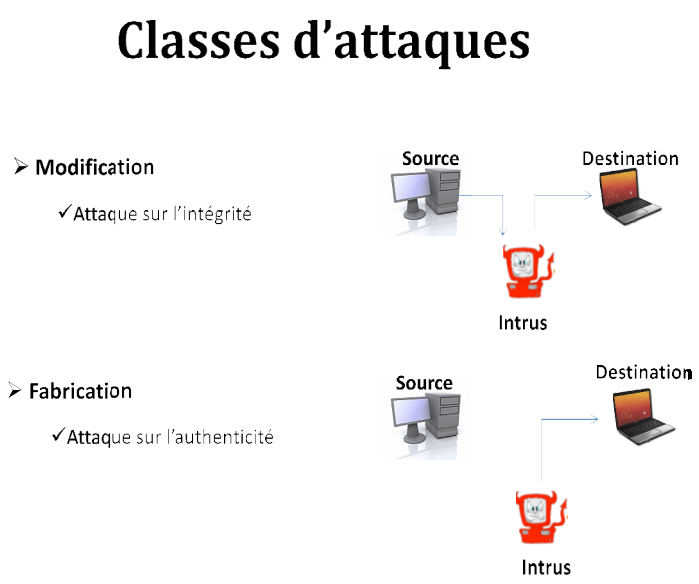


Figure 2 : Modification & Fabrication [4]

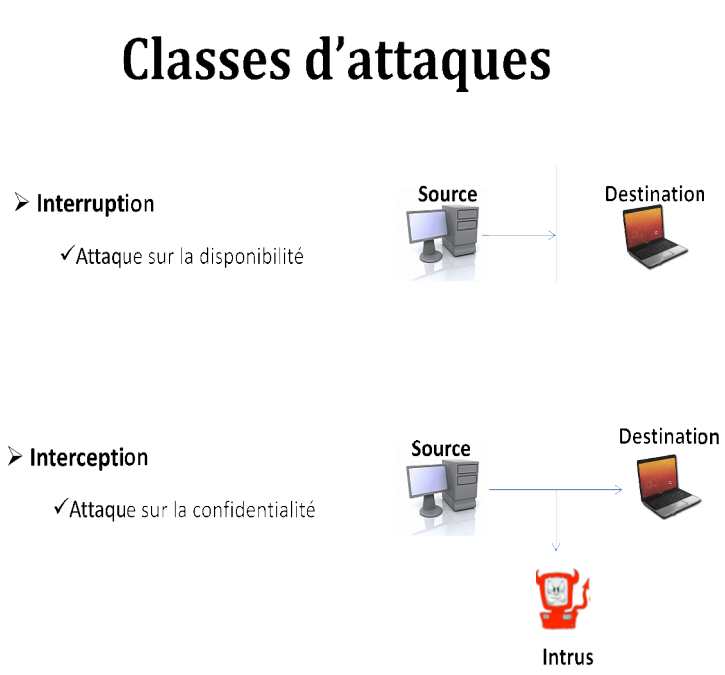


Figure 3 : Interruption & Interception [4]

Intrus :

Entité responsable d'une attaque de sécurité

- Contourne les mécanismes de sécurité mis en place.
- Devine ou décrypte les mots de passe utilisés pour protéger les ressources.

- Manipule et agit sur le fonctionnement interne des équipements de la victime (ordinateurs, routeurs, serveurs…etc.).
- Accède, de façon non autorisée, à des ressources internes de la victime.

I.5.5. Hacker :

En sécurité informatique, un **hacker** est un spécialiste disposant d'un savoir-faire exceptionnel dans la maîtrise de la sécurité informatique et donc des moyens de déjouer cette sécurité. Certains d'entre eux utilisent ce savoir-faire dans un cadre légal et d'autres l'utilisent hors-la-loi. Dans ce dernier cas, on parle de **pirates informatiques.**

- **Terminologie :**

Le jargon informatique classe les hackers en plusieurs catégories en fonction de leurs objectifs, de leur compétence et de la légalité de leurs actes [5]. Ce vocabulaire fait référence aux films de western, où le héros porte un chapeau blanc, et les méchants portent des chapeaux noirs. Par respect nous utiliserons le terme cracker et non hacker pour désigner ces personnes.

- Les **chapeaux blancs** ou *white hat* : professionnels de la sécurité informatique (consultants en sécurité, administrateurs réseaux...) effectuant des tests d'intrusions en accord avec leurs clients et la législation en vigueur afin de qualifier le niveau de sécurité de systèmes. Certains hackers se considèrent comme white hat alors qu'ils transgressent les lois [5], leur but étant de prévenir les responsables des failles de leurs systèmes. Certains d'entre eux s'infiltrent dans les systèmes de sécurités les plus coriaces juste pour la connaissance, pour se dire qu'ils savent le faire
- Les **chapeaux bleus** ou *blue hat* : consultants en sécurité informatique chargés de vérifier l'absence de bogues et de corriger d'éventuels exploits avant le lancement d'un système d'exploitation sur le marché. Le terme est notamment employé par Microsoft, désignant ses hackers et ingénieurs en sécurité informatique qui ont pour rôle de trouver les vulnérabilités de Windows. [4]
- Les **chapeaux noirs** ou *black hat* : créateurs de virus, cyber-espions, cyber-terroristes ou cyber-escrocs, agissant la plupart du temps hors-la-loi dans le but soit de nuire, de faire du profit ou d'obtenir des informations [4]. Ces hackers n'ont pas la même éthique que les White hats et sont souvent malveillants. Les plus malveillants sont alors appelés *crashers*.
- Les **chapeaux gris** ou *grey hat* : s'ils n'hésitent pas à pénétrer dans les systèmes sans y être autorisés, ils n'ont pas de mauvaises intentions. C'est souvent l'« exploit informatique » qui les motive, une façon de faire la preuve de leur agilité. Cette catégorie recouvre le large panel de personnes se situant entre le *black hat* et le *white hat*. [4]
- Les **script kiddies** ou *lamer*, littéralement « gamins qui utilisent des scripts » : sans grande compétence, ceux-ci piratent surtout par désir de se faire remarquer, en utilisant des programmes codés par d'autres [5]. Ces personnes ne sont pas à proprement parler des hackers, mais elles se considèrent généralement comme tels.
- Les **hacktivistes** : agissant afin de défendre une cause, ils n'hésitent pas à transgresser la loi pour attaquer des organisations afin de les paralyser ou d'obtenir des informations. [5]

Hacker, dans sa signification relayée par les médias de masse, se réfère aux chapeaux noirs (pirate informatique). Afin de lever l'ambiguïté sur le terme hacker, *cracker* est souvent utilisé pour désigner les *black hats*.

- **La culture du « Z »**

Voici un certain nombre de définitions propres au milieu « underground » :

- **Warez :** piratage de logiciels.
  - **Appz** (contraction de *applications* et *warez*) : piratage d'applications.
  - **Gamez** (contraction de *games* et *warez*) : piratage de jeux vidéos.
- **Serialz** (contraction de *serials* et *warez*) : il s'agit de numéros de série permettant d'enregistrer illégalement des copies de logiciels commerciaux.
- **Crackz** (contraction de *cracks* et *warez*) : ce sont des programmes écrits par des *crackers*, destinés à supprimer de manière automatique les systèmes de protection contre la copie des applications commerciales. [4]

I.5.6. Méthodes d'attaque portant atteinte à la sécurité du SI :

- **Destruction de matériels ou de supports :**

  ***Sabotage* :** il vise la mise hors service d'un SI ou de l'une de ses composantes en portant atteinte à l'intégrité des données et surtout à la disponibilité des services.[1]

- **Rayonnements électromagnétiques :**

  ***Brouillage* :** C'est une attaque de haut niveau qui vise à rendre le SI inopérant.

- **Écoute passive :**

  ***Écoute* :** Elle consiste à se placer sur un réseau informatique ou de télécommunication pour collecter et analyser les informations ou les trames qui y circulent
  ***Interception de signaux compromettants* :** l'attaquant tente de récupérer un signal électromagnétique pour l'interpréter et en déduire des informations utilisables.
  ***Cryptanalyse* :** L'attaque de données cryptées est réalisée par interception et analyse des cryptogrammes circulant lors d'une communication [1] ou obtenus par une source quelconque.

- **Vol :**

  ***Fraude physique* :** elle consiste à accéder à l'information par copie illégale des supports physiques (bandes magnétiques, disquettes, disques classiques ou optiques, listings rangés ou abandonnés imprudemment dans les bureaux, armoires, tiroirs...)
  ***Vol de matériels* :** concerne les ordinateurs et en particulier les ordinateurs portables.
  ***Analyse de supports recyclés ou mis au rebut* :** "fouille" des poubelles ou des archives d'une organisation ou détournement des processus de maintenance. [2]

- **Divulgation :**

***Hameçonnage ou filoutage (Phishing)* :** désigne l'obtention d'information confidentielle (comme des codes d'accès ou des mots de passe) en prétextant une fausse demande ou en faisant miroiter un pseudo-avantage auprès d'un utilisateur ciblé.[4]
***Chantage* :** menace exercée vis-à-vis d'une personne privée ou d'une organisation en vue d'extorquer une information "sensible".

- **Émission d'une information sans garantie d'origine :**

***Canular (Hoax)* :** vise à désinformer en annonçant l'arrivée d'un événement de nature imaginaire mais censé être fortement perturbateur voire catastrophique (virus).

- **Piégeage du logiciel :**

***Bombe* :** Programme dormant dont l'exécution est conditionné par l'occurrence d'un événement ou d'une date.
***Virus* :** Programme malicieux capable de faire fonctionner des actions nuisibles pour le SI, et éventuellement de se répandre par réplication à l'intérieur d'un SI. Les conséquences sont le plus souvent la perte d'intégrité des données d'un SI, la dégradation voire l'interruption du service fourni. [7]
***Ver* :** Programme malicieux qui a la faculté de se déplacer à travers un réseau qu'il cherche à perturber en le rendant totalement ou partiellement indisponible. [7]
***Piégeage du logiciel* :** Des fonctions cachées sont introduites à l'insu des utilisateurs à l'occasion de la conception, fabrication, transport ou maintenance du SI.
***Exploitation d'un défaut (bug)* :** Les logiciels en particulier les logiciels standards les plus répandus comportent des failles de sécurité qui constituent autant d'opportunité d'intrusion indésirables.
***Canal caché* :** Type d'attaque de très haut niveau permettant de faire fuir des informations en violant la politique de sécurité du SI. Les menaces peuvent concerner 4 types de canaux cachés : Canaux de stockage, Canaux temporels, Canaux de raisonnement, Canaux dits de "fabrication". [1]
***Cheval de Troie* :** C'est un programme ou un fichier introduit dans un SI et comportant une fonctionnalité cachée connue seulement de l'agresseur. L'utilisation d'un tel programme par l'utilisateur courant permet à l'attaquant de contourner les contrôles de sécurité en se faisant passer pour un utilisateur interne. [1]
***Réseau de robots logiciels (Botnet)* :** réseau de robots logiciels installés sur des machines aussi nombreuses que possible. Les robots se connectent sur des serveurs IRC (Internet Relay chat) [4] au travers desquels ils peuvent recevoir des instructions de mise en œuvre de fonctions non désirées. (envoi de spams, vol d'information, participation à des attaques de saturation ...).
***Logiciel espion (spyware)*:** est installé sur une machine dans le but de collecter et de transmettre à un tiers des informations sans que l'utilisateur en ait connaissance.
***Facticiel* :** logiciel factice disposant de fonctions cachées.

- **Saturation du Système informatique :**

***Perturbation* :** Vise à fausser le comportement du SI ou à l'empêcher de fonctionner comme prévu (saturation, dégradation du temps de réponse, génération d'erreurs).
***Saturation* :** Attaque contre la disponibilité visant à provoquer un déni de service (remplissage forcé d'une zone de stockage ou d'un canal de communication).

***Pourriel (spam)* :** Envoi massif d'un message non sollicité vers des utilisateurs n'ayant pas demandé à recevoir cette information. Cet usage non forcément hostile contribue cependant à la pollution et à la saturation des systèmes de messagerie.

- **Utilisation illicite des matériels :**

***Détournement d'utilisation normale* :** Utilise un défaut d'implantation ou de programmation de manière à faire exécuter à distance par la machine victime un code non désiré, voire malveillant.
***Fouille* :** En cas de mauvaise gestion des protections informatiques, celles-ci peuvent être contournées et laisser accéder aux fichiers de données par des visiteurs non autorisés.
***Mystification* :** Simulation du comportement d'une machine pour tromper un utilisateur légitime et s'emparer de son nom et mot de passe.
***Trappe* :** Fonctionnalité utilisée par les développeurs pour faciliter la mise au point de leurs programmes. Lorsqu'elle n'est pas enlevée avant la mise en service du logiciel, elle peut être repérée et servir de point de contournement des mesures de sécurité.
***Asynchronisme* :** Ce mode de fonctionnement crée des files d'attente et des sauvegardes de l'état du système. Ces éléments peuvent être détectés et modifiés pour contourner les mesures de sécurité.
***Souterrain* :** Attaque ciblée sur un élément supportant la protection du SI et exploitant une vulnérabilité existant à un niveau plus bas que celui utilisé par le développeur pour concevoir/tester sa protection. [4]
***Salami* :** Comportement d'un attaquant qui collecte des informations de manière parcellaire et imperceptible, afin de les synthétiser par la suite en vue d'une action rapide. (méthode fréquemment utilisée pour les détournements de fonds). [A1]
***Inférence sur les données* :** L'établissement d'un lien entre un ensemble de données non sensibles peut permettre dans certains cas de déduire quelles sont les données sensibles.

- **Altération des données :**

***Interception* :** C'est un accès avec modification des informations transmises sur les voies de communication avec l'intention de détruire les messages, de les modifier, d'insérer des nouveaux messages, de provoquer un décalage dans le temps ou la rupture dans la diffusion des messages.
***Balayage (scanning)*:** La technique consiste à envoyer au SI des informations afin de détecter celles qui provoquent une réponse positive. Par suite l'attaquant peut analyser les réponses reçues pour en dégager des informations utiles voire confidentielles (noms des utilisateurs et profil d'accès)

- **Abus de Droit :**

***Abus de droit* :** caractérise le comportement d'un utilisateur bénéficiaire de privilèges systèmes et/ou applicatifs qui les utilise pour des usages excessifs, pouvant conduire à la malveillance.

- **Usurpation de Droit :**

***Accès illégitimes* :** Lorsqu'une personne se fait passer occasionnellement pour une autre en usurpant son identité.
Déguisement : Désigne le fait qu'une personne se fait passer pour une autre de façon durable et répétée en usurpant son identité, ses privilèges ou les droits d'une personne visée. [1]
***Rejeu* :** Variante du déguisement qui permet à un attaquant de pénétrer un SI en envoyant une séquence de connexion d'un utilisateur légitime et enregistrée à son insu.
Substitution : Sur des réseaux comportant des terminaux distants, l'interception des messages de connexion-déconnexion peut permettre à un attaquant de continuer une session régulièrement ouverte sans que le système ne remarque le changement d'utilisateur.
***Faufilement* :** Cas particulier où une personne non autorisée franchit un contrôle d'accès en même temps qu'une personne autorisée. [A1]

- **Reniement d'actions :**

Le reniement (ou répudiation) consiste pour une partie prenante à une transaction électronique à nier sa participation à tout ou partie de l'échange d'informations, ou à prétendre avoir reçu des informations différentes (message ou document) de ceux réputés avoir été réalisés dans le cadre du SI.

I.6. Objectifs de la sécurité :

- Prévention

Prendre des mesures afin d'empêcher des attaques.

- Détection

Prendre des mesures afin de détecter quand, comment, par qui une attaque a été réalisée et les actifs ou les biens qui ont été endommagés.

- Réaction

Prendre des mesures après une attaque de sécurité afin de pouvoir restaurer les biens et les actifs, ou réduire l'impact de l'attaque.

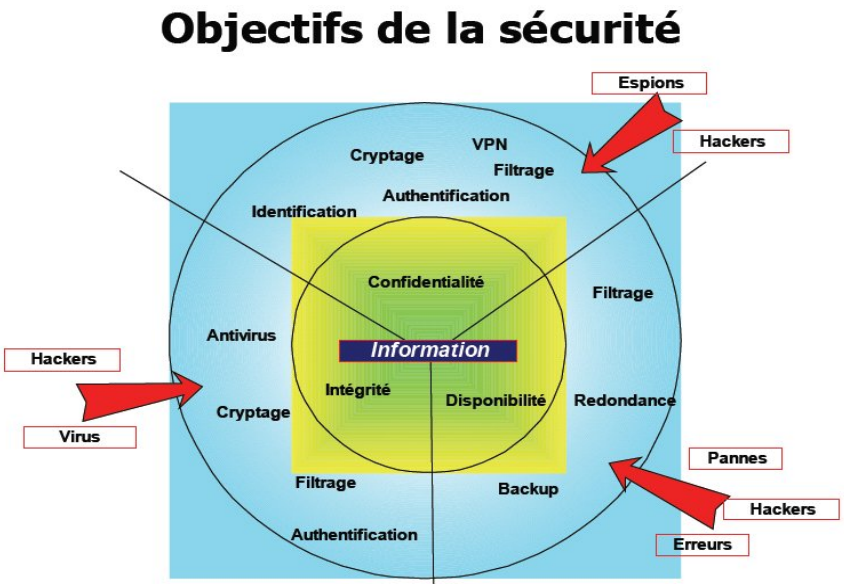


Figure 4 : Objectifs de la sécurité

I.7. Mécanismes et services de sécurité :

I.7.1. Mécanismes de sécurité :

Mécanismes conçus pour détecter, empêcher ou récupérer suite à une attaque de sécurité.

- ***Cryptage*** **:**
  - ✓ Utilisation d'algorithmes mathématiques pour transformer les messages en une forme inintelligible.
  - ✓ La transformation dépend d'un algorithme et de zéro à plusieurs clés.

- ***Signature numérique*** **:**
  - ✓ Ajout d'informations cryptées à une unité de données afin de prouver la source et l'intégrité de cette unité de données.

- ***Échange d'authentification*** **:**
  - ✓ Mécanisme assurant l'identité d'une entité à travers un échange d'information.

- ***Notarisation*****:**
  - ✓ Utilisation d'une tierce partie afin de confirmer l'identité de l'émetteur et du receveur d'un message.

- ***Horodatage (Timestamping)*** **:**
  - ✓ Inclusion d'une date et d'un temps correct dans un message.

- ***Autres mécanismes*** **:**
  - ✓ *Traffic Padding* : Mécanisme qui génère de fausses informations sur le réseau pour rendre l'analyse de trafic plus difficile.
  - ✓ Détection d'intrusions : Repérer les activités suspectes ou anormales sur le réseau.

- ✓ Pare-feu (filtrage): autoriser et interdire certains types de messages à circuler dans le réseau.
- ✓ Antivirus : empêcher les codes malveillants de s'exécuter.

I.7.2. Services de sécurité :

Services améliorant la sécurité du traitement de données et du transfert d'informations. Ces services s'opposent aux attaques de sécurité et font utiliser des mécanismes de sécurité.

- ➢ **Services de sécurité : Authentification**
- ✓ S'assurer que l'origine du message soit correctement identifiée
- ✓ Assurer le receveur que le message émane de la source qui prétend avoir envoyé ce message.
- ✓ Assurer l'authenticité des entités participantes: chacune des entités est celle qui prétende l'être.
- ✓ Empêcher la perturbation de la connexion par une tierce partie qui se fait passer pour une entité légitime (émission ou réception non autorisée).

Mécanismes utilisés: Cryptage, signature numérique, Notarisation.

- ➢ **Services de sécurité: Contrôle d'accès**
- ✓ Empêcher l'utilisation non autorisée d'une ressource (serveur, application, etc.).
- ✓ Définir qui a le droit d'accéder aux ressources.
- ✓ Déterminer sous quelles conditions ceci peut avoir lieu ?
- ✓ Défini ce qu'une entité est autorisée de faire lors de l'accès à une ressource.

Mécanismes utilisés: Authentification, signature numérique, pare-feu, mécanismes propres aux OS.

- ➢ **Services de sécurité: Confidentialité**
- ✓ Protection des données transmises contre les attaques passives, et protection des flux de données contre l'analyse.
- ✓ Préservation du secret des données transmises. Seulement les entités communicantes sont capables d'observer les données.

Il existe plusieurs niveaux de confidentialité :

- ✓ Protection de toutes les données échangées tout au long d'une connexion.
- ✓ Protection des données contenues au niveau d'un seul bloc de donnée.
- ✓ Protection de quelques champs des données échangées (pour une connexion ou un seul bloc de donnée).
- ✓ Protection de l'information (source, destination, etc.) qui peut être déduite à partir de l'observation des flux de données échangés. [2]

Mécanisme utilisé: Cryptage,

- ➢ **Services de sécurité: Intégrité**

- ✓ Détecter si les données ont été modifiées depuis la source vers la destination.
- ✓ Service orienté connexion: Protection contre la duplication, la destruction, l'insertion, la modification, le rejeu, le reclassement, etc.
- ✓ Service non orienté connexion: Protection contre la modification uniquement.

Mécanismes utilisés: cryptage, signature numérique, contrôle d'accès, contrôle d'intégrité.

- ➢ **Services de sécurité: Non répudiation**
- ✓ Empêche l'émetteur ou le receveur de nier avoir transmis ou reçu un message.
- ✓ Non répudiation d'envoi: Le destinataire prouve qu'une source déterminée vient d'émettre le message en question.
- ✓ Non répudiation de réception: L'émetteur prouve que son message a été reçu effectivement par la destination prétendue.

Mécanismes utilisés : signature numérique, notarisation

- ➢ **Services de sécurité: La disponibilité**
- ✓ la propriété qu'un système ou une ressource du système soit accessible et utilisable suite à la demande d'une entité autorisée.
- ✓ protège un système pour assurer sa disponibilité.
- ✓ Particulièrement contre des attaques de dénie de service.
- ✓ Dépend d'autres services comme le contrôle d'accès, l'authentification, …etc.

Mécanismes utilisés : Filtrage (pare-feu), antivirus, contrôle d'accès.

I.8. Conclusion :

Dans ce chapitre nous avons présenté, d'une manière générale, les concepts de base de la sécurité à savoir les critères de sécurité, menaces, risques et vulnérabilités. Nous avons vu aussi les méthodes d'attaques et les mécanismes de sécurité. Ces deux derniers seront largement étudiés et détaillés dans les prochains chapitres.

Dans le chapitre suivant, nous parlerons des différentes techniques d'attaques qui pèsent sur un système informatique.

Chapitre II : Techniques et types d'attaques

II.1. Introduction :

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Une « **attaque** » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

Les motivations des attaques peuvent être de différentes sortes :

- ✓ Obtenir un accès au système.
- ✓ Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- ✓ Recueillir des informations personnelles sur un utilisateur.
- ✓ Récupérer des données bancaires.
- ✓ S'informer sur l'organisation (entreprise de l'utilisateur).
- ✓ Troubler le bon fonctionnement d'un service.
- ✓ Utiliser le système de l'utilisateur comme « rebond » pour une attaque.
- ✓ Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

II.2. Niveaux de risque :

Les systèmes informatiques mettent en œuvre différentes composantes, allant de l'électricité pour alimenter les machines au logiciel exécuté via le système d'exploitation et utilisant le réseau. [2]

Les attaques peuvent intervenir à chaque maillon de cette chaîne, pour peu qu'il existe une vulnérabilité exploitable. Le schéma ci-dessous rappelle très sommairement les différents niveaux pour lesquels un risque en matière de sécurité existe :

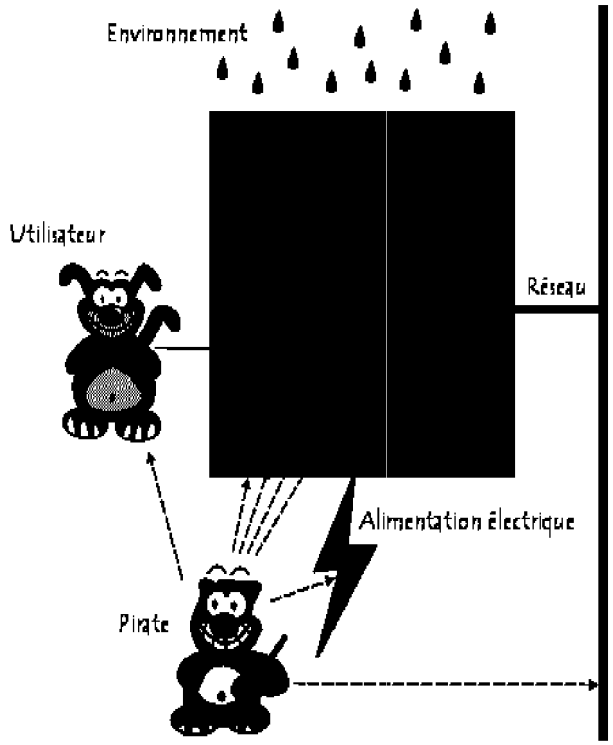


Figure 5 : niveaux de risque

II.3. Les grandes classes d'attaques :

- **Attaques visant l'authentification :**
  - ✓ ***Déguisement (Mascarade)***

Pour rentrer dans un système on essaye de piéger des usagers et de se faire passer pour quelqu'un d'autre:

Exemple: simulation d'interface système sur écran, simulation de terminal à carte bancaire.

- **Attaques visant l'intégrité des données :**
  - ✓ ***Modification de messages, de données***

Une personne non autorisée, un usager ou même un agent autorisé s'attribuent des avantages illicites en modifiant un fichier, un message (le plus souvent cette modification est réalisée par programme et entre dans la catégorie suivante).

Exemple : modification des données sur un serveur Web.

- **Attaques visant l'intégrité du flux de données :**
  - ✓ **Répétition ("replay")**

Espionnage d'une interface, d'une voie de communication (téléphonique, réseau local) pour capter des opérations (même cryptées elles peuvent être utilisables). [8]

- ✓ **Répétition de l'opération pour obtenir une fraude**

Exemple: Plusieurs fois la même opération de crédit d'un compte bancaire.

- **Attaques visant l'intégrité des programmes :**
  - ✓ **Modification des programmes**

***Les modifications à caractère frauduleux* :**

Pour s'attribuer par programme des avantages.

Exemple: virement des centimes sur un compte.

***Les modifications à caractère de sabotage* :**

Pour détruire avec plus ou moins de motivations des systèmes ou des données.

Deux types de modifications :

a) Infections informatiques à caractère unique

Bombe logique ou cheval de Troie.

Dans un programme normal on introduit un comportement illicite mis en action par une condition de déclenchement ou trappe (la condition, le moment ou l'on bascule d'un comportement normal à anormal).

Exemples: licenciement de l'auteur du programme.

b) Infections auto reproductrices

Il s'agit d'une infection informatique simple (du type précédent) **qui contient de plus une partie de recopie** d'elle même afin d'en assurer la propagation.

***Virus* :** à action brutale.

Ver : à action lente (détruisant progressivement les ressources d'un système).

- **Attaques visant la confidentialité :**

Les attaques ayant pour but le vol d'information via un réseau par **espionnage des transmissions de données** (espion de ligne, accès aux données dans des routeurs et des serveurs Internet)

- ✓ **Canaux cachés**
- ✓ **Analyse de trafic**

On observe le trafic de messages échangés pour en déduire des informations sur les décisions de quelqu'un.

Exemples:

Bourse : augmentation des transactions sur une place financière.

Militaire : le début de concentration entraîne un accroissement de trafic important.

- ✓ **Inférence**

On obtient des informations confidentielles à partir d'un faisceau de questions autorisées (et d'un raisonnement visant à faire ressortir l'information).

- **Attaques visant la disponibilité (déni de service) :**
  - ✓ **Attaque par violation de protocole**

Erreur très rare en fonctionnement normal et non supportées par le protocole.

- ✓ **Attaque par saturation**

Envoi de messages trop nombreux provoquant un écroulement des systèmes et réseaux.

Les attaques peuvent êtres également classées en attaques passives ou actives

- **Attaque passive**
  - ✓ Ne modifie pas le contenu de l'information ;
  - ✓ Tente de collecter ou d'utiliser des informations relatives au système, mais elle n'affecte pas les ressources du système ;
  - ✓ Très difficile à détecter mais assez facile à sécuriser (cryptage). [8]

Deux catégories essentielles d'attaques passives :

- ✓ ***Interception des messages* :**

En vue de tirer des informations pertinentes ou compromettantes (mots de passes, informations confidentielles, …etc.).

- ✓ ***Analyse de trafic* :**

En vue de comprendre l'architecture du réseau et de déceler les points faibles et les ressources importantes à attaquer.

- **Attaque actives**
  - ✓ Entraine la modification de l'information ou la création de fausses informations.
  - ✓ Il est difficile d'empêcher les attaques actives de façon absolue à moins de protéger physiquement tous les moyens et chemins de communications en même temps.

Quatre catégories essentielles d'attaques actives :

- ✓ ***Mascarade* :** Une entité prétend être une entité différente afin d'obtenir des privilèges.
- ✓ ***Rejeu (Replay)* :** capture passive des données et leurs transmission ultérieure en vue de réaliser des actions non autorisées.
- ✓ ***Modification* :** Altération, destruction, ou injection dans un message échangé en vue de produire un effet non souhaité ou non autorisé.
- ✓ ***Déni de service* :** Empêcher ou inhiber l'utilisation normale des moyens de communications.

II.4. Logiciel malveillant :

II.4.1. Dé inition:

Un **logiciel malveillant** (en anglais, ***malware***) est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté. De nos jours, le terme *virus* est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les malwares englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces [5]. La catégorie des virus informatiques, qui a longtemps été la plus répandue, a cédé sa place aux chevaux de Troie en 2005. [1]

II.4.2. Classification

Les logiciels malveillants peuvent être classés en fonction des trois mécanismes suivants :

- le **mécanisme de propagation** (par exemple, un *ver* se propage sur un réseau informatique en exploitant une faille applicative ou humaine) ;
- le **mécanisme de déclenchement** (par exemple, la *bombe logique* comme la bombe logique surnommée *vendredi 13* se déclenche lorsqu'un évènement survient) ;
- la **charge utile** (par exemple, le *virus* Tchernobyl tente de supprimer des parties importantes du BIOS, ce qui bloque le démarrage de l'ordinateur infecté).

La classification n'est pas parfaite, et la différence entre les classes n'est pas toujours évidente. Cependant, c'est aujourd'hui la classification standard la plus couramment adoptée dans les milieux internationaux de la sécurité informatique. [1]

- ***Les virus :*** Les **virus** sont capables de se répliquer, puis de se propager à d'autres ordinateurs en s'insérant dans d'autres programmes ou des documents légitimes appelés « hôtes ». Ils se répartissent ainsi : virus de secteur d'amorçage ; de fichier ; de macro ; et de script. Certains intègrent des rootkits [6]. Les virus peuvent s'avérer particulièrement dangereux et endommager plus ou moins gravement les machines infectées.
- ***Les vers :*** Les **vers** (*worm*) sont capables d'envoyer une copie d'eux-mêmes à d'autres machines. Ils peuvent être classés selon leur technique de propagation : les vers de courrier électronique ; Internet ; IRC ; les vers de réseau ; et ceux de partage de fichiers [7] . Certains, comme le ver *I Love You*, ont connu une expansion fulgurante.
- ***Les chevaux de Troie :*** Les **chevaux de Troie** (*Trojan horse*) sont divisés en plusieurs sous-catégories, et comprennent notamment les portes dérobées, les droppers, les notificateurs, les logiciels espions (dont les keyloggers) etc. Ils ont chacun des objectifs spécifiques. Certains chevaux de Troie utilisent également des rootkits pour dissimuler leur activité.[5]
- ***Autres menaces :*** D'autres menaces existent. Elles ne sont pas dangereuses en elles-mêmes pour la machine, mais servent à installer des infections ou à réaliser des attaques DNS. Il s'agit des outils de déni de service (DoS et DDoS), des exploits, inondeurs, *nukers*, du *pharming*, et des programmes qui servent à créer des logiciels malveillants, en particulier les *virtools*, les générateurs polymorphes, ou les crypteurs de fichiers. Les publiciels (*adware*) et les rogues (rançongiciels ou riskwares) ne sont pas non plus directement dommageables pour la machine. Il s'agit de programmes utilisant des techniques de mise en marché (ouverture de fenêtres intempestives, enregistrement automatique dans la barre URL, modification des liens référencés) bien souvent contraires à l'éthique.[5]

Certains éléments, qui ne sont pas à l'origine conçus pour être malveillants, sont parfois utilisées à des fins illégales et/ou compromettantes. Il s'agit notamment des composeurs, téléchargeurs, enregistreurs de frappes, serveurs FTP, mandataires (proxy), Telnet et Web,

clients IRC, canulars, utilitaires de récupération de mots de passe, outils d'administration à distance, décortiqueurs et moniteurs.

II.4.3. Liste des logiciels malveillants :

II.4.3.1. Cheval de Troie :

- **Définition :**

Un **cheval de Troie** (*Trojan Horse* en anglais) est un logiciel d'apparence légitime, conçu pour exécuter des actions à l'insu de l'utilisateur. En général, il utilise les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée (fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel qui permet à un pirate informatique de prendre, à distance, le contrôle de l'ordinateur) [5] . Les chevaux de Troie informatiques sont programmés pour être installés de manière invisible, notamment pour corrompre l'ordinateur hôte. La principale différence entre les virus, les vers et les chevaux de Troie est que ces derniers ne se répliquent pas. Ils sont divisés en plusieurs sous-classes comprenant entre autres les portes dérobées, les logiciels espions, les injecteurs, etc. On peut en trouver sur des sites malveillants ou autres. Cela dépend de ce que l'utilisateur télécharge.

- **Types et modes opératoires :**

Les chevaux de Troie se répartissent en plusieurs sous-catégories, et ont chacune leur mode de fonctionnement :

- Les **portes dérobées** sont les plus dangereux et les plus répandus des chevaux de Troie. Il s'agit d'un utilitaire d'administration à distance permettant à l'attaquant de prendre le contrôle des ordinateurs infectés via un LAN ou Internet [5]. Leur fonctionnement est similaire à ceux des programmes d'administration à distance légitimes à la différence que la porte dérobée est installée et exécutée sans le consentement de l'utilisateur. Une fois exécutée, elle surveille le système local de l'ordinateur et n'apparait que rarement dans le journal des applications actives [4]. Elle peut notamment envoyer, réceptionner, exécuter, supprimer des fichiers ou des dossiers, ainsi que redémarrer la machine. Son objectif est de récupérer des informations confidentielles, exécuter un code malicieux, détruire des données, inclure l'ordinateur dans des réseaux de bots, etc. Les portes dérobées combinent les fonctions de la plupart des autres types de chevaux de Troie. Certaines variantes de portes dérobées sont capables de se déplacer, mais uniquement lorsqu'elles en reçoivent la commande de l'attaquant.

Dans un logiciel, une **porte dérobée** (de l'anglais *backdoor*, littéralement *porte de derrière*) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel.

L'introduction d'une porte dérobée dans un logiciel à l'insu de son utilisateur transforme le logiciel en cheval de Troie

- Les **chevaux de Troie PSW** recherchent les fichiers système qui contiennent des informations confidentielles (comme les mots de passe, les détails du système, les

adresses IP, les mots de passe pour les jeux en ligne, etc.) [5] puis envoient par mail les données recueillies à la personne malintentionnée.

- Les **chevaux de Troie cliqueurs** redirigent les utilisateurs vers des sites Web ou d'autres ressources Internet. Pour cela, ils peuvent notamment détourner le fichier *hosts* (sous Windows). Ils ont pour but d'augmenter le trafic sur un site Web, à des fins publicitaires ; d'organiser une attaque par déni de service ; ou de conduire le navigateur web vers une ressource infectée (par des virus, chevaux de Troie, etc.). [8]
- Les **chevaux de Troie droppers** installent d'autres logiciels malveillants à l'insu de l'utilisateur. Le dropper contient un code permettant l'installation et l'exécution de tous les fichiers qui constituent la charge utile [8]. Il l'installe sans afficher d'avertissement ni de message d'erreur (dans un fichier archivé ou dans le système d'exploitation). Cette charge utile renferme généralement d'autres chevaux de Troie et un canular (blagues, jeux, images, etc.) qui, lui, a pour but de détourner l'attention de l'utilisateur ou de lui faire croire que l'activité de l'injecteur est inoffensive.
- Les **chevaux de Troie proxy** servent de serveur proxy. Ils sont particulièrement utilisés pour diffuser massivement des messages électroniques de spam.
- Les **chevaux de Troie espions** sont des logiciels espions et des programmes d'enregistrement des frappes, qui surveillent et enregistrent les activités de l'utilisateur sur l'ordinateur, puis transmettent les informations obtenues (frappes du clavier, captures d'écran, journal des applications actives, etc.) à l'attaquant.
- Les **chevaux de Troie notificateurs** sont inclus dans la plupart des chevaux de Troie. Ils confirment à leurs auteurs la réussite d'une infection et leur envoient (par mail ou ICQ) des informations dérobées sur l'ordinateur attaqué (adresse IP, ports ouverts, adresses de courrier électronique, etc.). [5]
- Les **bombes d'archives** sont des fichiers archivés infectés, codés pour saboter l'utilitaire de décompression (par exemple, Winrar ou Winzip) qui tente de l'ouvrir. Son explosion entraîne le ralentissement ou le plantage de l'ordinateur, et peut également noyer le disque avec des données inutiles. Ces bombes sont particulièrement dangereuses pour les serveurs. [5]

- **Exemples de Cheveux de Troie :** BotnetStorm Worm, SubSeven, XXXDial,

II.4.3.2. Logiciel espion :

- **Définition :**

Un **logiciel espion** (aussi appelé **mouchard** ou **espiogiciel** ; en anglais ***spyware***) est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance [8]. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

Le terme de *Logiciel espion*, dont l'usage est préconisé par la commission générale de terminologie et de néologie en France, contrairement à l'anglicisme *spyware* ou au terme québécois *espiogiciel*, est une traduction du mot anglais *spyware*, qui est une contraction de *spy* (espion) et *software* (logiciel).

- **Enregistreur de frappe :**

Un **enregistreur de frappe** (en anglais, *keylogger*) est un logiciel espion ou un périphérique qui espionne électroniquement l'utilisateur d'un ordinateur. Le but de cet outil est

varié, et peut se présenter sous des airs de légitimité [8], mais il ne peut être assuré qu'en espionnant l'intimité informatique de l'utilisateur.

Le terme *keylogger* est parfois utilisé pour parler de l'espionnage des périphériques d'entrée/sortie, bien que ces espions puissent être nommés spécifiquement en fonction du périphérique visé, comme les *mouseloggers* pour la souris.

- **Exemples de logiciels espion :** CoolWebSearch, Copy9, Cydoor, FinFisher, Gator, Magic Lantern, New.net, Phorm, SaveNow, XXXDial

II.4.3.3. Rootkit :

- **Définition :**

Un **rootkit** (le nom « outil de dissimulation d'activité » est également utilisé), parfois simplement « kit », est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible, à la différence d'autres logiciels malveillants. Le terme peut désigner la technique de dissimulation ou plus généralement un ensemble particulier d'objets informatiques mettant en œuvre cette technique. [9]

Pour l'« attaquant », l'utilité d'un rootkit est soit de mettre à disposition des ressources système (temps processeur, connexions réseaux, etc.) sur une, voire plusieurs machines (voir *infra*), parfois en utilisant la « cible » comme intermédiaire pour une autre attaque ; soit d'espionner, d'accéder aux données stockées ou en transit sur la machine cible.

- **Exemples de Rootkit :** Autorooter, NProtect, GameGuard,

II.4.3.4. Ver informatique :

- **Définition :**

Un **ver informatique** est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

- **Mode opératoire :**

Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction. [7]

L'objectif d'un ver n'est pas seulement de se reproduire. Le ver a aussi habituellement un objectif malfaisant, par exemple :

- espionner l'ordinateur où il se trouve ;
- offrir une porte dérobée à des pirates informatiques ;
- détruire des données sur l'ordinateur où il se trouve ou y faire d'autres dégâts ;
- envoyer de multiples requêtes vers un serveur Internet dans le but de le saturer (déni de service).

L'activité d'un ver a souvent des effets secondaires comme :

- le ralentissement de la machine infectée ;
- le ralentissement du réseau utilisé par la machine infectée ;
- le plantage de services ou du système d'exploitation de la machine infectée.

➢ **Les classes de vers :**

- Vers de réseau ;
- Vers de courrier électronique ;
- Vers de messagerie instantanée ;
- Vers Internet ;
- Vers IRC ;
- Vers de réseaux de partage de fichiers.

➢ **Exemples :** Bagle, Blaster, Flame (ver informatique), I love you, Melissa (ver informatique), Morris (ver informatique), SQL Slammer, Stuxnet.

II.4.3.5. Virus informatique :

➢ **Définition :**

Un **virus informatique** est un automate auto réplicatif à la base non malveillant, mais aujourd'hui souvent additionné de code malveillant (donc classifié comme logiciel malveillant), conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes » [7] . Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB, etc.

Les virus font souvent l'objet de fausses alertes que la rumeur propage, encombrant les messageries [9]. Certaines d'entre elles, jouant sur l'ignorance en informatique des utilisateurs, leur font parfois détruire des éléments totalement sains du système d'exploitation.

➢ **Différents types de virus :**

Le **virus classique** est un morceau de programme, souvent écrit en assembleur, qui s'intègre dans un programme normal, le plus souvent à la fin, mais cela peut varier. Chaque fois que l'utilisateur exécute ce programme « infecté », il active le virus qui en profite pour aller s'intégrer dans d'autres programmes exécutables [7]. De plus, lorsqu'il contient une charge utile, il peut, après un certain temps (qui peut être très long) ou un évènement particulier, exécuter une action prédéterminée. Cette action peut aller d'un simple message anodin à la détérioration de certaines fonctions du système d'exploitation ou la détérioration de certains fichiers ou même la destruction complète de toutes les données de l'ordinateur. On parle dans ce cas de « bombe logique » et de « charge utile ».

Un **virus de boot** (ou virus de secteur d'amorçage) s'installe dans un des secteurs de boot d'un périphérique de démarrage, disque dur (le secteur de boot principal, le « *Master boot record* », ou celui d'une partition), disquette, ou autre [7]. Il remplace un chargeur d'amorçage (ou programme de démarrage ou « *bootloader* ») existant (en copiant l'original ailleurs) ou en créé un (sur un disque ou il n'y en avait pas) mais ne modifie pas un programme comme un

virus normal ; quand il remplace un programme de démarrage existant, il agit un peu comme un virus « *prepender* » (qui s'insère au début), mais le fait d'infecter aussi un périphérique vierge de tout logiciel de démarrage le distingue du virus classique, qui ne s'attaque jamais à « rien ».

Les **macrovirus** qui s'attaquent aux macros de logiciels de la suite Microsoft Office (Word, Excel, etc.) grâce au VBA de Microsoft. Par exemple, en s'intégrant dans le modèle normal.dot de Word, un virus peut être activé à chaque fois que l'utilisateur lance ce programme. [6]

Les **virus-vers**, apparus aux environs de l'année 2003, ayant connu un développement fulgurant dans les années qui suivirent, sont des virus classiques car ils ont un programme hôte [6]. Mais s'apparentent aux vers (en anglais « *worm* ») car :

- Leur mode de propagation est lié au réseau, comme des vers, en général via l'exploitation de failles de sécurité.
- Comme des vers, leur action se veut discrète, et non-destructrice pour les utilisateurs de la machine infectée.
- Comme des vers, ils poursuivent des buts à visée large, tels que l'attaque par saturation des ressources ou attaque DoS (*Denial of Service*) d'un serveur par des milliers de machines infectées se connectant simultanément. [7]

Les **virus de type batch**, apparu à l'époque où MS-DOS était le système d'exploitation en vogue, sont des virus « primitifs » [7] . Bien que capables de se reproduire et d'infecter d'autres fichiers batch, ils sont lents et ont un pouvoir infectant très faible.

- **Caractéristiques :**

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

***Le polymorphisme* :** le virus est chiffré et la routine de déchiffrement est capable de changer certaines de ses instructions au fil des réplications afin de rendre plus difficile la détection par l'antivirus.

***Le métamorphisme* :** contrairement au chiffrement simple et au polymorphisme, où le corps du virus ne change pas et est simplement chiffré, le métamorphisme permet au virus de modifier sa structure même et les instructions qui le composent.

***La furtivité* :** le virus « trompe » le système d'exploitation (et par conséquent les logiciels antivirus) sur l'état des fichiers infectés. Des rootkits permettent de créer de tels virus [9]. Par exemple, l'exploitation d'une faille de sécurité au niveau des répertoires permet de masquer l'existence de certains fichiers exécutables ainsi que les processus qui leur sont associés.

- **Fichier de test Eicar :**

Le **fichier de test Eicar** est une chaîne de caractères, écrite dans un fichier informatique, destiné à tester le bon fonctionnement des logiciels antivirus.

Pour tester un antivirus, il suffit de créer un fichier texte de 68 octets contenant les caractères suivants :

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Ce fichier ne contient pas de virus mais une signature qui doit être détectée par le logiciel antivirus si celui-ci est basé sur une méthode de recherche par signature. Il peut être renommé en fichier .COM, c'est un fichier exécutable MS-DOS valide inoffensif affichant "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!". Propriété inusuelle pour un programme en langage machine, le code ne contient que des caractères ASCII affichables, ce qui lui permet d'être saisi dans un éditeur de texte standard. Cela est rendu possible par l'utilisation de code automodifiable. [1]

- **Exemples de virus :** AIDS (virus informatique), Bliss (virus), Bugbear, Cabir, CommWarrior, Doomboot, Koobface, Virut.

II.4.3.6. Rogue (logiciel malveillant) :

Un faux logiciel de sécurité, comme un antivirus ou un anti-spyware. Ce type de programme est vendu par des sociétés éditrices de logiciels, lesquelles avaient auparavant provoqué chez leurs clients potentiels de l'étonnement, du stress ou invoqué des menaces imaginaires. Il s'agit d'une pratique de marketing non éthique. [5]

Une tactique habituelle est de convaincre un utilisateur que son ordinateur contient un logiciel malveillant, puis lui suggérer de télécharger un logiciel pour l'éliminer, logiciel payant. L'infection est le plus souvent fictive et le logiciel est inutile ou est lui-même malveillant.

- **Fonctionnement :**

Les symptômes causés par une infection par un rogue sont :

- Défaillances système ;
- Fenêtres pop-ups et fausses alertes ;
- Connexion de l'ordinateur à Internet sans votre autorisation ;
- Annonces publicitaires.

II.4.3.7. Bombe de décompression :

Une **bombe de décompression** est un type de logiciel malveillant qui consiste en un fichier compressé dont la décompression mobilise tellement de ressources qu'il peut faire geler le système. Elle peut aussi être utilisée pour occuper l'antivirus pendant qu'un virus plus traditionnel est introduit.

- **Bombe simple (ou bombe à données répétées) :**

Il s'agit d'un simple fichier compressé, placé à un endroit quelconque du disque dur, d'une taille relativement légère (n'excédant pas une dizaine de mégaoctets), qui contient après décompression des données d'une taille beaucoup plus importante (plusieurs gigaoctets). Pour ce faire, on remplit intégralement, sur plusieurs gigaoctets, un fichier binaire d'une même donnée (0 ou 1). Ainsi, une fois compressé, il sera très léger. [8]

Lors d'une analyse ce fichier va être analysé par l'antivirus pour peu que celui-ci supporte l'analyse de fichiers compressés (ce qui est le cas pour pratiquement tous les antivirus à ce jour). Pour cela, l'antivirus va devoir extraire l'archive dans une zone temporaire, afin de les analyser un par un. Là est la source du problème : lorsqu'on extrait ce fichier ce sont plusieurs gigaoctets de données qui doivent être extraits et copiés dans cette zone. Ce processus de décompression occupe toute la mémoire temporaire qui lui est dédiée et créé un déni de service (ou DoS) en accaparant toutes les ressources du processeur.

Certains antivirus sont cependant capables de reconnaître les bombes de décompression avant qu'elles ne soient décompressées.

- **Bombe complexe :**

Une bombe complexe est un fichier compressé dont l'en-tête est incorrect.

- **Bombe simple à série de fichiers :**

Cette bombe est en fait plusieurs bombes identiques les unes dans les autres. Certains formats de compression permettent de compresser un grand nombre de fois un même fichier dans une seule archive sans augmenter la taille finale de l'archive [8]. On compressera donc plusieurs milliers voire millions de bombes simples dans un fichier compressé, et la taille de la bombe finale différera peu de celle d'une unique bombe simple. La taille des fichiers décompressés lors de l'explosion de la bombe peut alors atteindre plusieurs centaines de pétaoctets.

- **Autres bombes :**

Ce problème touchant tous les types de fichiers compressés, il est ainsi possible de créer des bombes à image (*picture bomb* : un seul pixel est répété sur une image de plusieurs millions de pixels de côté).

II.4.3.8. Bombe logique :

En sécurité informatique, une **bombe logique** est la partie d'un virus, d'un cheval de Troie ou de tout autre logiciel malveillant qui contient les fonctions destinées à causer des dommages dans l'ordinateur infecté.

La bombe logique est donc la *charge utile* du logiciel malveillant. On l'oppose donc aux fonctions destinées à la réplication du code ou à sa diffusion.

II.4.3.9. Browser hijacker :

Un ***browser hijacker*** (anglicisme signifiant littéralement « pirate de navigateur ») est un type de logiciel malveillant capable de modifier, à l'insu d'un utilisateur, certaines options de son navigateur web telles que la page de démarrage, la page d'erreur, ou la page de recherche, afin de le forcer à consulter d'autres pages que celles qui étaient définies auparavant. [5]

CoolWebSearch, apparu en 2003, est l'un des premiers et des plus connus.

Ils agissent sur la base de registre.

II.4.3.10. Composeur (en anglais, *dialer*) :

est un terme générique qui désigne un logiciel permettant de raccorder un ordinateur à un autre ordinateur, à un appareil électronique, au réseau Internet ou à un autre réseau numérique.

- **Fonctionnement :**

Le *composeur* tire son nom du fait qu'il *compose* un numéro de téléphone pour connecter l'ordinateur sur lequel il se trouve à un autre appareil. [9]

Tous les composeurs peuvent composer un numéro de téléphone. Cependant, certains contiennent des fonctions supplémentaires, ce qui fait que les différents composeurs ont des fonctions bien différentes. Certains sont légaux et d'autres sont des logiciels malveillants

II.4.3.11. Facticiel :

Un **facticiel** (mot valise composé des mots « logiciel » et « factice ») est un type de logiciel malveillant qui se fait passer pour un logiciel, le plus souvent de sécurité ou de performance système [9]. Les facticiels se présentent comme des logiciels de sécurité en reproduisant leur apparence, et renforcent l'impression de légitimité par le fait qu'ils sont souvent payants. Ils peuvent permettre le détournement de données personnelles. Le nombre d'installations de ce type de logiciel malveillant a été estimé à 43 millions par an en 2009.

II.4.3.12. Hacktool :

Est un logiciel malveillant utilisé par des hackers dans différents buts. Il inclut entre autres des balayeurs de port, des renifleurs, un enregistreur de frappe et des outils d'envoi de pourriel (*spam*) [9]. On retrouve ce logiciel sous différents noms : *HackTool*, *HackTools*, *Hack Tool*, *Hack Tools*, *Hacktool Spammer*, *Flooder*, *Hacking Tool* ou encore *Hacking Tools*.

- **Conséquences**

Ce logiciel, en général non viral, présente peu de risques pour l'internaute, bien qu'il puisse se faire voler ses mots de passe.

Cependant, il peut être utilisé pour une attaque à venir, aussi bien du réseau que de la machine infectée.

II.4.3.13. Security Master AV :

Security Master AV est un logiciel malveillant qui usurpe l'identité d'un antivirus, mais qui en est en fait un cheval de Troie sous Windows. [11]

Il peut enlever la permission d'accéder à certains fichiers système et créer certains problèmes dans l'ordinateur.

I1.4.3.14. Wabbit :

Un **wabbit** est un type de logiciel malveillant qui s'autoréplique. Contrairement aux virus, il n'infecte pas les programmes ni les documents. Contrairement aux vers, il ne se propage pas par les réseaux. [11]

En plus de s'autorépliquer rapidement, les wabbits peuvent avoir d'autres effets malveillants. Un exemple de wabbit est la bombe fork, du nom de la commande Unix exploitée : fork. [A1]

II.5. Exploit :

Un **exploit** (ou **exploiteur**) est, dans le domaine de la sécurité informatique, un élément de programme permettant à un individu ou un logiciel malveillant d'exploiter une faille de sécurité informatique dans un système d'exploitation ou dans un logiciel que ce soit à distance, *remote exploit*, ou sur la machine sur laquelle cet exploit est exécuté, *local exploit* ; ceci, afin de prendre le contrôle d'un ordinateur ou d'un réseau, de permettre une augmentation de privilège d'un logiciel ou d'un utilisateur, ou d'effectuer une attaque par déni de service. [4]

Le terme provient de l'anglais *exploit*, 'exploiter' (ici une faille de sécurité). L'usage est de le prononcer à l'anglaise « *explo-ï-te* » et non « *exploi* » comme en français.

II.6. Technique d'attaques :

II.6.1. Vol de session TCP (TCP session hijacking) :

Le « **vol de session TCP** » (également appelé *détournement de session TCP* ou en anglais *TCP session hijacking*) est une technique consistant à intercepter une session TCP initiée entre deux machine afin de la détourner. [11]

Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

- **Source-routing**

La méthode de détournement initiale consistait à utiliser l'option *source routing* du protocole IP. Cette option permettait de spécifier le chemin à suivre pour les paquets IP, à l'aide d'une série d'adresses IP indiquant les routeurs à utiliser. [9]]

En exploitant cette option, le pirate peut indiquer un chemin de retour pour les paquets vers un routeur sous son contrôle.

- **Attaque à l'aveugle**

Lorsque le source-routing est désactivé, ce qui est le cas de nos jours dans la plupart des équipements, une seconde méthode consiste à envoyer des paquets « à l'aveugle » (en anglais « blind attack »), sans recevoir de réponse, en essayant de prédire les numéros de séquence. [9]

- **Man in the middle**

Enfin, lorsque le pirate est situé sur le même brin réseau que les deux interlocuteurs, il lui est possible d'écouter le réseau et de « faire taire » l'un des participants en faisant planter sa machine ou bien en saturant le réseau afin de prendre sa place. [9]

II.6.2. Usurpation d'adresse IP (en anglais : *IP spoofing*) :

Une autre attaque très utilisée est l'usurpation d'adresse IP, elle consiste à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.
En outre, Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement, ce qui rend très difficile l'identification de la source de cette attaque. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une *mascarade* (déguisement) de l'adresse IP au niveau des paquets émis. [1]
La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (***le pare-feu)***. En effet, un système pare-feu (en anglais *firewall*) fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines internes au réseau.

II.6.3 .ARP poisoning :

L'*ARP spoofing*, ou ***ARP poisoning***, est une technique utilisée en informatique pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP, les cas les plus répandus étant les réseaux Ethernet et Wi-Fi [11]. Cette technique permet à l'attaquant de détourner des flux de communications transitant entre une machine cible et une passerelle : routeur, box, etc. L'attaquant peut ensuite écouter, modifier ou encore bloquer les paquets réseaux.

L'ARP spoofing est une étape de l'attaque de l'homme du milieu.

II.6.4. L'analyse de réseau :

Un « **analyseur réseau** » (appelé également *analyseur de trames* ou en anglais *sniffer*, traduisez « renifleur ») est un dispositif permettant d'« écouter » le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent. [1]

En effet, dans un réseau non commuté, les données sont envoyées à toutes les machines du réseau. Toutefois, dans une utilisation normale les machines ignorent les paquets qui ne leur sont pas destinés. Ainsi, en utilisant l'interface réseau dans un mode spécifique (appelé généralement *mode promiscuous*) il est possible d'écouter tout le trafic passant par un adaptateur réseau (une carte réseau ethernet, une carte réseau sans fil, etc.).

- **Utilisation du sniffer**

Un sniffer est un formidable outil permettant d'étudier le trafic d'un réseau. Il sert généralement aux administrateurs pour diagnostiquer les problèmes sur leur réseau ainsi que pour connaître le trafic qui y circule. Ainsi les détecteurs d'intrusion (*IDS*, pour *intrusion detection system*) sont basés sur un sniffeur pour la capture des trames, et utilisent une base de données de règles (*rules*) pour détecter des trames suspectes.

Malheureusement, comme tous les outils d'administration, le sniffer peut également servir à une personne malveillante ayant un accès physique au réseau pour collecter des informations.

Ce risque est encore plus important sur les réseaux sans fils car il est difficile de confiner les ondes hertziennes dans un périmètre délimité, si bien que des personnes malveillantes peuvent écouter le trafic en étant simplement dans le voisinage. [8]

La grande majorité des protocoles Internet font transiter les informations en clair, c'est-à-dire de manière non chiffrée. Ainsi, lorsqu'un utilisateur du réseau consulte sa messagerie via le protocole POP ou IMAP, ou bien surfe sur internet sur des sites dont l'adresse ne commence pas par HTTPS, toutes les informations envoyées ou reçues peuvent être interceptées. C'est comme cela que des sniffers spécifiques ont été mis au point par des pirates afin de récupérer les mots de passe circulant dans le flux réseau.

II.6.5. Balayage de port :

Le **balayage de port** (*port scanning* en anglais) est une technique servant à rechercher les ports ouverts sur un serveur de réseau.

Cette technique est utilisée par les administrateurs des systèmes informatiques pour contrôler la sécurité des serveurs de leurs réseaux. La même technique est aussi utilisée par les pirates informatiques pour tenter de trouver des failles dans des systèmes informatiques. Un balayage de port (*port scan* ou *portscan* en anglais) effectué sur un système tiers est généralement considéré comme une tentative d'intrusion, car un balayage de port sert souvent à préparer une intrusion. [8]

Les balayages de ports se font habituellement sur le protocole TCP ; néanmoins, certains logiciels permettent aussi d'effectuer des balayages UDP. Cette dernière fonctionnalité est beaucoup moins fiable, UDP étant orienté sans connexion, le service ne répondra que si la requête correspond à un modèle précis variant selon le logiciel serveur utilisé.

Avant de lancer une attaque sur un réseau TCP / IP, l'attaquant a besoin d'identifier les systèmes qui sont connectés au réseau de sa cible et donc quelles adresses sont actives, comment la topologie du réseau est construite et quels services sont disponibles. [11]
Etant donné une plage d'adresses réseau, le mappeur de réseau va envoyer des paquets à chaque adresse possible afin de déterminer celles des machines qui sont effectivement dans ce réseau. En envoyant un simple PING (un paquet ICMP), l'outil de mapping utilisé peut déterminer si un serveur ou une machine est connectée au réseau en question [9]. Aujourd'hui il existe des outils de mapping qui peuvent envoyer des paquets SYN qui permettent d'établir une connexion et si jamais le serveur est à l'écoute alors le paquet SYN déclenche un ACK (acknowledgement) si le port est ouvert ou il envoie un message " Port injoignable " si le port est fermé.
Indifféremment, le port étant ouvert ou fermé la réponse indique si la machine est à l'écoute et donc existe dans ce réseau, ainsi l'attaquant pourra orienter et raffiner ses attaques.
Un scanner de port permet d'identifier les ports ouverts dans un système.
Il y a 65 535 ports TCP et 65 535 ports UDP dans un système dont quelques uns sont ouverts et la plupart sont fermés, par exemple le port 80 TCP est très utilisé par les serveurs web, port 25 TCP est utilisé dans le net par « server-to-server mail exchange ». En utilisant un scanner de port, l'attaquant va envoyer des paquets à tous les ports du système cible et voir ceux qui répondent et donc savoir lesquels sont ouverts et quels services sont en cours d'exécution. [3]

II.6.6. Dépassement de tampon :

Un **dépassement de tampon** ou **débordement de tampon** (en anglais, ***buffer overflow***) est un bug par lequel un processus, lors de l'écriture dans un tampon, écrit à l'extérieur de l'espace alloué au tampon, écrasant ainsi des informations nécessaires au processus.

Lorsque le bug se produit non intentionnellement, le comportement de l'ordinateur devient imprévisible. Il en résulte souvent un blocage du programme, voire de tout le système. [11]

Le bug peut aussi être provoqué intentionnellement et être exploité pour violer la politique de sécurité d'un système. Cette technique est couramment utilisée par les pirates. La stratégie de l'attaquant est alors de détourner le programme bugué en lui faisant exécuter des instructions qu'il a introduites dans le processus.

- **Cas particulier de dépassement de tampon : débordement de nombre entier**

Il est fréquent d'allouer dynamiquement des tableaux de structure de données, ce qui implique le calcul de la taille totale du tableau : taille_d' un_élément * nombre_d'éléments. Un tel produit peut donner un nombre trop grand pour être enregistré dans l'espace normalement alloué à un nombre entier. On a alors un dépassement d'entiers et le produit est tronqué, ce qui donne un résultat erroné plus petit que le résultat attendu [11]. La zone mémoire allouée au tableau est alors de taille inférieure à ce qu'on pense avoir alloué. C'est un cas très particulier de dépassement de tampon, qui peut être utilisé par un attaquant.

- **Autres types de dépassement de tampon**

Il existe plusieurs autres types de dépassements de tampon. Ces failles de sécurité ont été couramment exploitées depuis le début des années 2000, en particulier dans OpenSSH et dans les bibliothèques de lecture de pratiquement tous les types d'image.

- **Dépassement de tas**

En plus des techniques de piratage basées sur les dépassements de tampon, il existe d'autres techniques de piratage qui exploitent le débordement d'autres variables contenues dans d'autres parties de la mémoire. En particulier, plusieurs attaques exploitent le débordement des variables du tas. Ces dépassements sont appelés dépassement de tas (en anglais, *heap overflow*).

II.6.7. Le spam :

Le ***spam***, **courriel indésirable** ou **pourriel** est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. [10]

Le terme « polluriel » est plutôt utilisé pour définir les messages inutiles, souvent provocateurs et n'ayant aucun lien avec le sujet de discussion, qui sont diffusés massivement sur de nombreux forums ou groupes de nouvelles, ce qui entraîne une pollution des réseaux.

- **Contenu et objectifs du spam :**

- Le spam contient généralement de la publicité. Les produits les plus vantés sont les services pornographiques, les médicaments (le plus fréquemment les produits de « dopage sexuel » ou, des hormones utilisées dans la lutte contre le vieillissement ou encore pour la perte de poids), le crédit financier, les casinos en ligne, les montres de contrefaçon, les diplômes falsifiés et les logiciels craqués.
- Des escrocs envoient également des propositions prétendant pouvoir vous enrichir rapidement : travail à domicile, conseil d'achat de petites actions (penny stock). [10]
- Les lettres en chaînes peuvent aussi être qualifiées de spam.
- Parfois aussi, mais de plus en plus rarement, il s'agit de messages d'entreprises ignorantes de la nétiquette qui y voient un moyen peu coûteux d'assurer leur promotion.
- Certains messages indiquant qu'un courriel n'est pas arrivé à destination peuvent également être qualifiés de spam lorsque le message d'origine n'a pas été envoyé par vous même mais par exemple par un virus se faisant passer pour vous.
- Enfin la dernière forme de spam, l'hameçonnage (ou « *phishing* », de l'anglais, terme dérivé de « *fishing* », la pêche à la ligne), consiste à tromper le destinataire en faisant passer un courriel pour un message de sa banque ou d'un quelconque service protégé par mot de passe [A3]. Le but est de récupérer les données personnelles des destinataires (notamment des mots de passe, un numéro de carte bancaire) en les attirant sur un site factice enregistrant toutes leurs actions.

Les spams encombrent le réseau, et font perdre du temps à leurs destinataires.
Le spam est une des causes les plus importantes de perte de temps et de contamination de virus et logiciels malveillants dans le monde.

- **Vecteurs du spam :**

Le spam peut s'attaquer à divers médias électroniques : les courriels, les forums de discussion de Usenet, les moteurs de recherche, les wikis, les messageries instantanées, les blogues.

II.6.8. Mail-bombing :

Le **mail-bombing** ou **bombardement de messagerie** ou encore **bombarderie** est une technique d'attaque visant à saturer une boîte aux lettres électronique par l'envoi en masse de messages quelconques par un programme automatisé [10]. On utilise les termes de *mail-bomber* pour caractériser l'action de faire du *mail-bombing* (de saturer de messages/courriels) et de *mail-bomb* pour le courrier reçu sous cette forme et dans ce but.

II.6.9. Le canular informatique (*hoax* en anglais) :

Un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes. Ils encombrent le réseau, et font perdre du temps à leurs destinataires [8]. Dans certains cas, ils incitent l'utilisateur à effectuer des manipulations dangereuses sur son poste (suppression d'un fichier prétendument lié à un virus par exemple).

II.7. Attaques cryptographiques :

II.7.1. Attaque de l'homme du milieu :

L'**attaque de l'homme du milieu** (**HDM**) ou *man in the middle attack* (**MITM**) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet de l'internaute lambda [4]. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. L'attaque « homme du milieu » est particulièrement applicable dans le protocole original d'échange de clés Diffie-Hellman, quand il est utilisé sans authentification [9]. Avec authentification, Diffie-Hellman est en revanche invulnérable aux écoutes du canal, et est d'ailleurs conçu pour cela.

- **Le problème de l'échange des clés :**

Un des problèmes majeurs lorsque deux personnes veulent échanger des données chiffrées, est celui de la transmission des clés : pour s'assurer d'être les seuls à connaître ces informations secrètes, les correspondants doivent pouvoir les échanger de façon confidentielle.

Dans le cadre de la cryptographie symétrique, il faut disposer d'un canal sécurisé qui lui-même nécessite une clé pour être établi. Le problème entre ainsi dans un cercle vicieux.

Dans le cadre de la cryptographie asymétrique, il a été en partie résolu. Les deux personnes possèdent chacune leur clé publique (qui sert à chiffrer) et leur clé privée (qui sert à déchiffrer). Ainsi, seules les clés publiques sont échangées, ce qui ne nécessite pas un canal sécurisé. Même si quelqu'un réussissait à intercepter et à lire ces clés publiques, elles ne lui seraient d'aucune utilité pour déchiffrer, en partant du principe que l'algorithme de chiffrement est cryptographiquement sûr.

La résolution complète du problème nécessite une Infrastructure à clés publiques. En effet, dans la cryptographie asymétrique, il serait possible à un tiers, *l'homme du milieu*, de remplacer les clés publiques échangées par ses propres clefs publiques. Il lui serait alors possible d'intercepter tous les messages, de les déchiffrer avec ses clefs privées et de les re-signer aussi [9]. Le rôle d'une Infrastructure à clés publiques est donc de certifier que les clefs publiques correspondent bien aux deux parties.

- **L'attaque de l'homme du milieu :**

L'attaque de l'homme du milieu ajoute comme condition supplémentaire que l'attaquant ait la possibilité non seulement de lire, mais de modifier les messages. Dans ce cas, même le chiffrement asymétrique est vulnérable [4]. Toutefois, il est généralement très difficile de pouvoir modifier l'intégralité des messages qui transitent.

Le but de l'attaquant est de se faire passer pour l'un (voire les 2) correspondants, en utilisant, par exemple :

- l'ARP *Spoofing* : c'est probablement le cas le plus fréquent. Si l'un des interlocuteurs et l'attaquant se trouvent sur le même réseau local, il est possible, voire relativement aisé, pour l'attaquant de forcer les communications à transiter par son ordinateur en se faisant passer pour un « relais » (routeur, passerelle) indispensable [4]. Il est alors assez simple de modifier ces communications ;

- le DNS *Poisoning* : L'attaquant altère le ou les serveur(s) DNS des parties de façon à rediriger vers lui leurs communications sans qu'elles s'en aperçoivent ;
- l'analyse de trafic afin de visualiser d'éventuelles transmissions non cryptées ;
- le déni de service : l'attaquant peut par exemple bloquer toutes les communications avant d'attaquer un parti. L'ordinateur ne peut donc plus répondre et l'attaquant a la possibilité de prendre sa place.

II.7.2. Attaque par relais :

Une **attaque par relais**, connu en anglais sous le nom de « relay attack », est un type d'attaque informatique, similaire à l'attaque de l'homme du milieu, dans lequel un attaquant ne fait que relayer mot pour mot un message d'un expéditeur vers un récepteur valide. [9]

Le but de l'attaque par relais est de pouvoir usurper l'identité ou les droits d'un utilisateur. Le pirate sera en mesure de contourner des systèmes de contrôle d'accès, de frauder des systèmes de paiement, de détourner des votes par bulletins électroniques, de s'introduire et de communiquer sur tout réseau sur lequel il ne serait normalement pas admis. Il pourra également accéder à des fichiers réservés ou inonder (Spam) des messageries de courriers électroniques.

II.7.3. Attaques par mots de passe :

II.7.3.1. L'attaque par dictionnaire :

Est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Elle consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire. Si ce n'est pas le cas, l'attaque échouera. [9]

Cette méthode repose sur le fait que de nombreuses personnes utilisent des mots de passe courants (par exemple : un prénom, une couleur ou le nom d'un animal). C'est pour cette raison qu'il est toujours conseillé de *ne pas utiliser de mot de passe comprenant un mot ou un nom*.

L'attaque par dictionnaire est une méthode souvent utilisée en complément de l'attaque par force brute qui consiste à tester, de manière exhaustive, les différentes possibilités de mots de passe. Cette dernière est particulièrement efficace pour des mots de passe n'excédant pas 5 ou 6 caractères.

II.7.3.2. Attaque par force brute :

L'**attaque par force brute** est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles.

Cette méthode en général considérée comme la plus simple concevable. Elle permet de casser tout mot de passe en un temps fini indépendamment de la protection utilisée, mais le temps augmente avec la longueur du mot de passe [9]. En théorie la complexité d'une attaque par force brute est une fonction exponentielle de la longueur du mot de passe, la rendant virtuellement impossible pour des mots de passe de longueur moyenne, mais en pratique des optimisations heuristiques peuvent donner des résultats dans des délais beaucoup plus courts.

Cette méthode est souvent combinée avec l'attaque par dictionnaire et par table arc-en-ciel pour trouver le secret plus rapidement.

II.7.4. La rétro-ingénierie :

En cryptographie, la rétroingénierie prend plusieurs formes avec des attaques cryptanalytiques. Le but est d'extraire des informations secrètes depuis la « boîte noire » symbolisant la procédure de chiffrement. Ces types d'attaques sont nommés attaques par canaux auxiliaires

II.7.5. Attaque par démarrage à froid (de l'anglais « *cold boot attack* ») :

En cryptographie, une **attaque par démarrage à froid** (de l'anglais « *cold boot attack* ») est une forme d'attaque par canal auxiliaire dans laquelle un cracker ayant un accès physique à un ordinateur est capable de récupérer les clefs de chiffrement d'une partition de disque dur après un démarrage à froid d'un système d'exploitation. L'attaque repose sur la rémanence des données inhérente aux mémoires électroniques de type DRAM ou SRAM pour récupérer l'information préalablement stockée et toujours lisible durant plusieurs secondes, après la coupure de l'alimentation, ou après avoir été retirées de la carte mère [11]

II.8. Attaques par Déni de service :

Une **attaque par déni de service** (*denial of service attack*, d'où l'abréviation **DoS**) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de :

- l'inondation d'un réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service à une personne en particulier.

L'attaque par déni de service peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web ou empêcher la distribution de courriel dans une entreprise. [8]

L'attaquant cracker n'a pas forcément besoin de matériel sophistiqué. Ainsi, certaines attaques DOS peuvent être exécutées avec des ressources limitées contre un réseau beaucoup plus grand et moderne. On appelle parfois ce type d'attaque « attaque asymétrique » (en raison de la différence de ressources entre les protagonistes) [11]. Un cracker avec un ordinateur obsolète et un modem lent peut ainsi neutraliser des machines ou des réseaux beaucoup plus importants.

Les attaques en déni de service se sont modifiées au cours du temps.

Tout d'abord, les premières n'étaient perpétrées que par un seul « attaquant » ; rapidement, des attaques plus évoluées sont apparues, impliquant une multitude de « soldats », aussi appelés « zombies ». On parle alors de DDoS (*distributed denial of service attack*) [8]. Ensuite, les attaques DoS et DDoS étaient perpétrées par des crackers seulement attirés par l'exploit et la renommée. Ainsi, certains crackers se sont spécialisés dans la « levée » d'armées de « zombies », qu'ils peuvent ensuite louer à d'autres crackers pour attaquer une cible particulière. Avec la forte augmentation du nombre d'échanges commerciaux sur Internet, le nombre de chantages au déni de service a très fortement progressé (un cracker lance une

attaque en DoS ou DDoS contre une entreprise et lui demande une rançon pour arrêter cette attaque).

- ***Dénis De Service distribués:***

Le DoS distribués est une version avancée du DoS, l'idée consiste à relayer les attaques depuis plusieurs machines compromises qui travaillent en coordination, et le système cible de l'attaque est appelé la victime principale tandis que les machines compromises sont appelées victimes secondaires ou des zombies, et celui qui lance l'attaque on l'appelle le maître. Il est très difficile de tracer cette attaque car elle provient de plusieurs machines en même temps.

Motivation : Compte tenu des performances actuelles des serveurs et de la généralisation des techniques de répartition de charge et de haute disponibilité, il est quasiment impossible de provoquer un déni de service simple comme décrit dans les sections précédentes. Il est donc souvent nécessaire de trouver un moyen d'appliquer un effet multiplicateur à l'attaque initiale.

- **Les protections contre les attaques de déni de service**

Les attaques par déni de service non distribuées peuvent être contrées en identifiant l'adresse IP de la machine émettant les attaques et en la bannissant au niveau du pare-feu ou du serveur. Les paquets IP provenant de la machine hostile sont dès lors rejetés sans être traités empêchant que le service du serveur ne soit saturé et ne se retrouve donc hors-ligne. [11]

Les attaques par déni de service distribuées sont plus difficiles à contrer. Le principe même de l'attaque par déni de service distribuée est de diminuer les possibilités de stopper l'attaque. Celle-ci émanant de nombreuses machines hostiles aux adresses différentes, bloquer les adresses IP limite l'attaque mais ne l'arrête pas. Thomas Longstaff de l'université Carnegie-Mellon explique à ce sujet que : « En réalité, la prévention doit plus porter sur le renforcement du niveau de sécurité des machines connectées au réseau [pour éviter qu'une machine puisse être compromise] que sur la protection des machines cibles [les serveurs Web] ». [8]

Une architecture répartie, composée de plusieurs serveurs offrant le même service gérés de sorte que chaque client ne soit pris en charge que par l'un d'entre eux, permet de répartir les points d'accès aux services et offre, en situation d'attaque, un mode dégradé (ralentissement) souvent acceptable.

Selon les attaques il est également possible de mettre un serveur tampon qui filtre et nettoie le trafic. Ce serveur, « *cleaning center* » permet en cas d'attaques de faire en sorte que les requêtes malveillantes ne touchent pas le serveur visé.

L'utilisation de SYN cookies est également une solution envisageable pour éviter les attaques de type SYN flood, mais cette approche ne permet pas d'éviter la saturation de la bande passante du réseau.

II.8.1. La technique dite « par réflexion » :

Le smurf est une attaque par rebond. Celle-ci permet à un pirate de causer un déni de service.

L'assaillant utilise l'IP spoofing pour envoyer des requêtes ICMP *echo request* (*ping*) à plusieurs machines qui vont alors servir de *rebonds*. Il utilise l'adresse IP source d'une machine qu'il veut mettre hors service pour envoyer ses requêtes. [8]
Toutes les machines répondront à l'adresse IP « spoofée » (usurpée).
La technique dite « attaque par réflexion » est basée sur l'utilisation de serveurs de diffusion (*broadcast*) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau.

Le scénario d'une telle attaque est le suivant :

- la machine attaquante envoie une requête *ping* (ping est un outil exploitant le protocole ICMP, permettant de tester les connexions sur un réseau en envoyant un paquet et en attendant la réponse) à un ou plusieurs serveurs de diffusion en falsifiant l'adresse IP source (adresse à laquelle le serveur doit théoriquement répondre) et en fournissant l'adresse IP d'une machine cible.
- le serveur de diffusion répercute la requête sur l'ensemble du réseau ;
- toutes les machines du réseau envoient une réponse au server de diffusion,
- le serveur broadcast redirige les réponses vers la machine cible.

Ainsi, lorsque la machine attaquante adresse une requête à plusieurs serveurs de diffusion situés sur des réseaux différents, l'ensemble des réponses des ordinateurs des différents réseaux vont être routées sur la machine cible

II.8.2. Écran bleu de la mort :

L'**écran bleu de la mort** aussi abrégé **BSoD** de l'anglais ***Blue Screen of Death*** se réfère à l'écran affiché par le système d'exploitation Microsoft Windows lorsqu'il ne peut plus récupérer une erreur système ou lorsqu'il est à un point critique d'erreur fatale [1]. Il y a deux types d'écrans d'erreur, dont l'un est l'écran bleu de la mort, qui a une signification d'erreur plus sérieuse que l'autre.

II.8.3. Fork bomb :

La **fork bomb** est une forme d'attaque par déni de service contre un système informatique utilisant la fonction fork. Elle est basée sur la supposition que le nombre de programmes et de processus pouvant être exécutés simultanément sur un ordinateur est limité.

La *fork bomb* fonctionne en créant autant de processus que possible. Ainsi, pour empêcher une *fork bomb*, il suffit simplement de limiter le nombre de processus pouvant être exécutés par un programme ou par un utilisateur. En permettant aux utilisateurs de non-confiance de lancer seulement un petit nombre de processus, le danger d'une *fork bomb*, intentionnelle ou non, est réduit [11]. Toutefois, cela n'empêche pas un groupe d'utilisateurs de collaborer pour consommer les emplacements processus, à moins que la limite totale des processus soit plus grande que la somme des limites des processus individuelles.

II.8.4. Le ping de la mort (en anglais *ping of death* ou PoD) :

Est une attaque historique de type déni de service réalisé par l'envoi de paquet ping malformé. Un ping a normalement une taille de 56 octets (soit 84 octets avec l'entête IP), or

certains systèmes n'étaient pas en mesure de traiter correctement les paquets plus gros que la taille maximale (65 535 octets) pouvant provoquer un crash de la machine cible.

II.8.5. Flooding:

Le ***flood*** ou ***flooding*** est une action généralement malveillante qui consiste à envoyer une grande quantité de données inutiles dans un réseau afin de le rendre inutilisable, par exemple en saturant sa bande passante ou en provoquant le plantage des machines du réseau dont le déni de service est la conséquence possible.

- **Ping flood :**

Un **ping flood** (ou ICMP flood) est une forme simple d'attaque par déni de service, où l'attaquant inonde le serveur cible de requêtes ping.

Ce type d'attaque ne réussit que si l'attaquant a plus de bande passante que sa victime (par exemple, un hacker avec une connexion Internet qui transmet 20 millions de bits par seconde et une victime avec une connexion Internet de 10 millions de bits par seconde). [5]

- **SYN flood :**

L'« **attaque SYN** » (appelée également « *TCP/SYN Flooding* ») est une attaque réseau par saturation (*déni de service*) exploitant le mécanisme de poignéee de main en trois temps (en anglais *Three-ways handshake*) du protocole TCP.

Le mécanisme de poignée de main en trois temps est la manière selon laquelle toute connexion « fiable » à internet (utilisant le protocole TCP) s'effectue. [8]

Lorsqu'un client établit une connexion à un serveur, le client envoie une requête SYN, le serveur répond alors par un paquet *SYN/ACK* et enfin le client valide la connexion par un paquet *ACK* (*acknowledgement*, qui signifie *accord* ou *remerciement*).

Une connexion TCP ne peut s'établir que lorsque ces 3 étapes ont été franchies. L'attaque SYN consiste à envoyer un grand nombre de requêtes SYN à un hôte avec une adresse IP source inexistante ou invalide. Ainsi, il est impossible que la machine cible reçoive un paquet *ACK*.

Les machines vulnérables aux attaques SYN mettent en file d'attente, dans une structure de données en mémoire, les connexions ainsi ouvertes, et attendent de recevoir un paquet *ACK*. Il existe un mécanisme d'expiration permettant de rejeter les paquets au bout d'un certain délai. Néanmoins, avec un nombre de paquets SYN très important, si les ressources utilisées par la machine cible pour stocker les requêtes en attente sont épuisées, elle risque d'entrer dans un état instable pouvant conduire à un plantage ou un redémarrage

II.9. Attaques web :

- **Vulnérabilité des services web :**

Les premières attaques réseau exploitaient des vulnérabilités liées à l'implémentation des protocoles de la suite TCP/IP. Avec la correction progressive de ces vulnérabilités, les

attaques se sont décalées vers les couches applicatives et en particulier le web, dans la mesure où la plupart des entreprises ouvrent leur système pare-feu pour le traffic destiné au web.

Le protocole HTTP (ou HTTPS) est le standard permettant de véhiculer les pages web par un mécanisme de requêtes et de réponses. Utilisé essentiellement pour transporter des pages web informationnelles (pages web statiques), le web est rapidement devenu un support interactif permettant de fournir des services en ligne [3]. Le terme d'« application web » désigne ainsi toute application dont l'interface est accessible à travers le web à l'aide d'un simple navigateur. Devenu le support d'un certain nombre de technologies (SOAP, Javascript, XML RPC, etc.), le protocole HTTP possède désormais un rôle stratégique certain dans la sécurité des systèmes d'information [1].

Dans la mesure où les serveurs web sont de plus en plus sécurisés, les attaques se sont progressivement décalées vers l'exploitation des failles des applications web.

Ainsi, la sécurité des services web doit être un élément pris en compte dès leur conception et leur développement.

- **Types de vulnérabilités :**

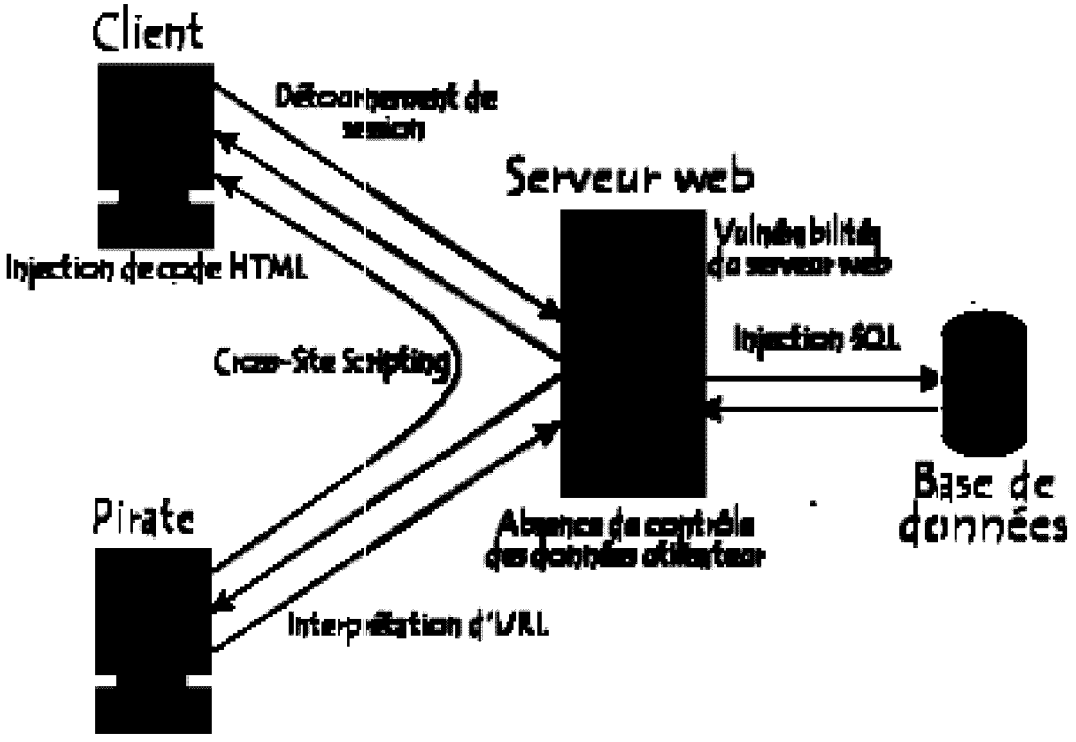


Figure 6 : Vulnérabilités Web

Les vulnérabilités des applications web peuvent être catégorisées de la manière suivante :

- Vulnérabilités du serveur web. Ce type de cas est de plus en plus rare car au fur et à mesure des années les principaux développeurs de serveurs web ont renforcé leur sécurisation ;

- Manipulation des URL, consistant à modifier manuellement les paramètres des URL afin de modifier le comportement attendu du serveur web ;
- Exploitation des faiblesses des identifiants de session et des mécanismes d'authentification ;
- Injection de code HTML et Cross-Site Scripting ;
- Injection de commandes SQL.

➢ **Impact des attaques web :**

Les attaques à l'encontre des applications web sont toujours nuisibles car elles donnent une mauvaise image de l'entreprise. Les conséquences d'une attaque réussie peuvent notamment être une des suivantes :

- Défacement de site web :un **défacement**, **défaçage** ou **défiguration** (*defacing* en anglais) est un anglicisme désignant la modification non sollicitée de la présentation d'un site web, à la suite du piratage de ce site. Il s'agit donc d'une forme de détournement de site Web par un hacker. [8]
- Vol d'informations.
- Modification de données, notamment modification de données personnelles d'utilisateurs.
- Intrusion sur le serveur web.

II.9.1. Cross-site scripting :

Le **cross-site scripting** (abrégé **XSS**), est un type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, permettant ainsi de provoquer des actions sur les navigateurs web visitant la page. Les possibilités des XSS sont très larges puisque l'attaquant peut utiliser tous les langages pris en charge par le navigateur (JavaScript, Java, Flash...) et de nouvelles possibilités sont régulièrement découvertes notamment avec l'arrivée de nouvelles technologies comme HTML5. Il est par exemple possible de rediriger vers un autre site pour du hameçonnage ou encore de voler la session en récupérant les cookies. [1]

Le cross-site scripting est abrégé XSS pour ne pas être confondu avec le CSS (feuilles de style), X se lisant « cross » (croix) en anglais.

➢ **Risques :**

L'exploitation d'une faille de type XSS permettrait à un intrus de réaliser les opérations suivantes :

- Redirection (parfois de manière transparente) de l'utilisateur (souvent dans un but de hameçonnage)
- Vol d'informations, par exemple sessions et cookies.
- Actions sur le site faillible, à l'insu de la victime et sous son identité (envoi de messages, suppression de données…)
- Rendre la lecture d'une page difficile (boucle infinie d'alertes par exemple).

Il est également possible de se protéger des failles de type XSS à l'aide d'équipements réseaux dédiés tels que les pare-feux applicatifs. Ces derniers permettent de filtrer l'ensemble des flux HTTP afin de détecter les requêtes suspectes.

II.9.2. Injection de commandes SQL :

Les attaques par **injection de commandes SQL** sont des attaques visant les sites web s'appuyant sur des bases de données relationnelles.

Dans ce type de sites, des paramètres sont passés à la base de données sous forme d'une requête SQL. Ainsi, si le concepteur n'effectue aucun contrôle sur les paramètres passés dans la requête SQL, il est possible à un pirate de modifier la requête afin d'accéder à l'ensemble de la base de données, voire à en modifier le contenu.

En effet, certains caractères permettent d'enchaîner plusieurs requêtes SQL ou bien ignorer la suite de la requête. Ainsi, en insérant ce type de caractères dans la requête, un pirate peut potentiellement exécuter la requête de son choix. [11]

Soit la requête suivante, attendant comme paramètre un nom d'utilisateur :

SELECT * FROM utilisateurs WHERE nom="$nom";

Il suffit à un pirate de saisir un nom tel que « toto" OR 1=1 OR nom ="titi » pour que la requête devienne la suivante :

SELECT * FROM utilisateurs WHERE nom="toto" OR 1=1 OR nom ="titi";

Ainsi, avec la requête ci-dessus, la clause WHERE est toujours réalisée, ce qui signifie qu'il retournera les enregistrements correspondant à tous les utilisateurs. [8]

- **Procédures stockées :**

De plus, certains systèmes de gestion de bases de données tel que *Microsoft SQL Server* possèdent des procédures stockées permettant de lancer des commandes d'administration. Ces procédures stockées sont potentiellement dangereuses dans la mesure où elles peuvent permettre à un utilisateur malintentionné d'exécuter des commandes du système, pouvant conduire à une éventuelle intrusion.

II.9.3. Attaques par manipulation d'URL :

L'URL (Uniform Resource Locator) d'une application web est le vecteur permettant d'indiquer la ressource demandée.
Il s'agit d'une chaîne de caractères ASCII imprimables qui se décompose en cinq parties :

- Le nom du protocole
- Identifiant et mot de passe
- Le nom du serveur
- Le numéro de port
- chemin d'accès à la ressource

- **Manipulation d'URL**

En manipulant certaines parties d'une URL, un pirate peut amener un serveur web à délivrer des pages web auxquelles il n'est pas censé avoir accès.

En effet, sur les sites web dynamiques les paramètres sont la plupart passés au travers de l'URL de la manière suivante :

http://cible/forum/index.php3?cat=2

Les données présentes dans l'URL sont créées automatiquement par le site et lors d'une navigation normale un utilisateur ne fait que cliquer sur les liens proposés par le site web. Ainsi, si un utilisateur modifie manuellement le paramètre, il peut essayer différentes valeurs, par exemple : [8]

http://cible/forum/index.php3?cat=6

Si le concepteur n'a pas anticipé cette éventualité, le pirate peut éventuellement obtenir un accès à un espace normalement protégé.
Par ailleurs, le pirate peut amener le site à traiter un cas inattendu, par exemple :

http://cible/forum/index.php3?cat=**********

Dans le cas ci-dessus, si le concepteur du site n'a pas prévu le cas où la donnée n'est pas un chiffre, le site peut entrer dans un état non prévu et révéler des informations dans un message d'erreur.

- **Tâtonnement à l'aveugle :**

Un pirate peut éventuellement tester des répertoires et des extensions de fichier à l'aveugle, afin de trouver des informations importantes. Voici quelques exemples classiques :

- Recherche de répertoires permettant d'administrer le site : [8]

http://cible/admin/
http://cible/admin.cgi

- Recherche de script permettant de révéler des informations sur le système distant :

http://cible/phpinfo.php3

- **Traversement de répertoires :**

Les attaques dites « de traversement de répertoires » (en anglais *directory traversal* ou *path traversal*) consistent à modifier le chemin de l'arborescence dans l'URL afin de forcer le serveur à accéder à des sections du site non autorisées.
Dans un cas classique, l'utilisateur peut être amené à remonter progressivement l'arborescence, notamment dans le cas où la ressource n'est pas accessible, par exemple : [8]

http://cible/base/test/ascii.php3
http://cible/base/test/
http://cible/base/

Sur les serveurs vulnérables, il suffit de remonter le chemin avec plusieurs chaînes du type « ../ » :

http://cible/../../../../repertoire/fichier

Des attaques plus évoluées consistent à encoder certains caractères :

- soit sous la forme d'encodage d'URL :

http://cible/..%2F..%2F..%2Frepertoire/fichier

- soit avec une notation Unicode :

http://cible/..%u2216..%u2216repertoire/fichier

II.10.Arnaques:

II.10.1. L'hameçonnage (*phishing* en anglais) :

Un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles.
C'est une technique de fraude mélangeant spamming (envoi en masse de messages à des adresses électroniques collectées illégalement ou composées automatiquement) et ingénierie sociale (comme l'usurpation d'identité) dans le but de subtiliser des informations sensibles aux victimes (identité complète, numéro de carte bancaire, identifiants d'accès à un site Internet, etc.). La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (banque, administration, etc.) afin de lui soutirer des renseignements personnels (mot de passe, numéro de carte de crédit, etc.). Le phishing peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques. [10]
Une attaque par phishing se présente souvent en deux temps : l'internaute reçoit en général un message de sa banque ou d'une autre société qui l'informe d'un problème de sécurité ou d'une autre action nécessitant qu'il se rende sur le site concerné et qui l'invite pour cela à cliquer sur un lien hypertexte. Or ce dernier ne conduit pas au site officiel mais vers une imitation souvent identique à l'original contrôlée par un individu malveillant, aussi si l'internaute clique sur le lien et saisit des informations elles seront transmises directement à l'escroc. D'autres variantes existent cependant, comme un formulaire à remplir intégré dans le message ou une demande de réponse par retour du courriel.

II.10.2. Loterie :

Vous recevez un courrier électronique indiquant que vous êtes l'heureux gagnant du premier prix d'une grande loterie d'une valeur de plusieurs (centaines de) milliers d'euros. Pour empocher le pactole il suffit de répondre à ce courrier.

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

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

II.10.3. Le scam :

Le « **scam** » (« ruse » en anglais), est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. L'arnaque du scam est issue du Nigéria, ce qui lui vaut également l'appellation « 419 » en référence à l'article du code pénal nigérian réprimant ce type de pratique. [9]

L'arnaque du scam est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds.

En répondant à un message de type scam, l'internaute s'enferme dans un cercle vicieux pouvant lui coûter de quelques centaines d'euros s'il mord à l'hameçon et même la vie dans certains cas.

En effet, deux cas de figures se présentent :

- Soit les échanges avec l'escroc se font virtuellement auquel cas celui-ci va envoyer quelques « documents officiels » pour rassurer sa victime et petit à petit lui demander d'avancer des frais pour des honoraires d'avocats, puis des frais de douanes, des frais de banque, etc.
- Soit la victime accepte, sous pression du cyberbandit, de se rendre dans le pays avec la somme en liquide auquel cas elle devra payer des frais pour pouvoir rester dans le pays, payer des frais de banque, soudoyer des hommes d'affaires, et ainsi de suite. Dans le meilleur des cas la victime rentre chez elle en avion délestée d'une somme d'argent non négligeable, dans le pire scénario plus personne ne la revoit...

II.10.4. Ingénierie sociale :

Le terme d'« **ingénierie sociale** » (en anglais « *social engineering* ») désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct.

L'ingénierie sociale est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs en se faisant passer pour une personne de la maison, un technicien, un administrateur, etc. [11]

D'une manière générale les méthodes d'ingénierie sociale se déroule selon le schéma suivant :

- Une phase d'approche permettant de mettre l'utilisateur en confiance, en se faisant passer pour une personne de sa hiérarchie, de l'entreprise, de son entourage ou pour un client, un fournisseur, etc.
- Une mise en alerte, afin de le déstabiliser et de s'assurer de la rapidité de sa réaction. Il peut s'agir par exemple d'un prétexte de sécurité ou d'une situation d'urgence ;

- Une diversion, c'est-à-dire une phrase ou une situation permettant de rassurer l'utilisateur et d'éviter qu'il se focalise sur l'alerte. Il peut s'agir par exemple d'un remerciement annonçant que tout est rentré dans l'ordre, d'une phrase anodine ou dans le cas d'un courrier électronique ou d'un site web, d'une redirection vers le site web de l'entreprise.

L'ingénierie sociale peut prendre plusieurs formes :

- Par téléphone,
- Par courrier électronique,
- Par courrier écrit,
- Par messagerie instantanée,
- etc.

II.11. Technique d'évasion :

Ces techniques permettent, par différentes méthodes, de cacher au système de détection (généralement un IDS) les informations nécessaires à la détection d'une attaque (ARP poisoning, spoofing, modifications des règles de l'IDS).

II.12. Autres techniques :

II.12.1. le cassage de logiciel (*Cracking* en version anglaise) :

Cette technique a pour but la modification d'un programme pour déjouer sa protection (en général pour permettre une utilisation complète, ou à durée illimitée) ;

II.12.2. Récupération de formulaire :

La **récupération de formulaire** (en anglais, *Form grabbing*) est une méthode criminelle utilisé par les pirates informatiques pour récupérer les diverses données des navigateurs. Elle est souvent confondue avec le *keylogger*, cette méthode intercepte l'envoi dans les navigateurs et collecte ainsi les données avant que celle ci soit envoyées sur internet. D'autres méthodes utilisent un add-on ou une barre d'outils malicieuse pour lire automatiquement les informations [5]. Ces méthodes sont très utilisées dans la récupération de données bancaires et d'autres données sensibles car ils récupèrent uniquement le nécessaire, le nom d'utilisateur et le mot de passe généralement. Il est beaucoup plus utilisé car il ne nécessite pas une vérification manuelle des logs comme un keylogger. C'est une méthode de plus en plus usitée sur le web. Le Malware le plus connu l'utilisant est Zeus, un botnet spécialisé sur les récupérations bancaires.

II.13. Méthodologie d'une intrusion sur un réseau :

Nous allons essayer d'expliquer la méthodologie généralement retenue par les pirates pour s'introduire dans un système informatique. En effet, la meilleure façon de protéger son système est de procéder de la même manière que les pirates afin de cartographier les vulnérabilités du système.

II.13.1. Méthodologie globale :

Les hackers ayant l'intention de s'introduire dans les systèmes informatiques recherchent dans un premier temps des **failles**, c'est-à-dire des *vulnérabilités* nuisibles à la sécurité du système, dans les protocoles, les systèmes d'exploitation, les applications ou même le personnel d'une organisation ! Les termes de **vulnérabilité**, de **brèche** ou en langage plus familier de **trou de sécurité** (en anglais *security hole*) sont également utilisés pour désigner les failles de sécurité. [8]

Pour pouvoir mettre en oeuvre un exploit (il s'agit du terme technique signifiant *exploiter une vulnérabilité*), la première étape du hacker consiste à récupérer le maximum d'informations sur l'architecture du réseau et sur les systèmes d'exploitations et applications fonctionnant sur celui-ci. La plupart des attaques sont l'oeuvre de *script kiddies* essayant bêtement des exploits trouvés sur internet, sans aucune connaissance du système, ni des risques liés à leur acte.

Une fois que le hacker a établi une cartographie du système, il est en mesure de mettre en application des exploits relatifs aux versions des applications qu'il a recensées. Un premier accès à une machine lui permettra d'étendre son action afin de récupérer d'autres informations, et éventuellement d'étendre ses privilèges sur la machine.

Lorsqu'un accès administrateur (le terme anglais *root* est généralement utilisé) est obtenu, on parle alors de compromission de la machine (ou plus exactement en anglais *root compromise*), car les fichiers systèmes sont susceptibles d'avoir été modifiés. Le hacker possède alors le plus haut niveau de droit sur la machine.

S'il s'agit d'un pirate, la dernière étape consiste à effacer ses traces, afin d'éviter tout soupçon de la part de l'administrateur du réseau compromis et de telle manière à pouvoir garder le plus longtemps possible le contrôle des machines compromises.

Le schéma suivant récapitule la méthodologie complète :

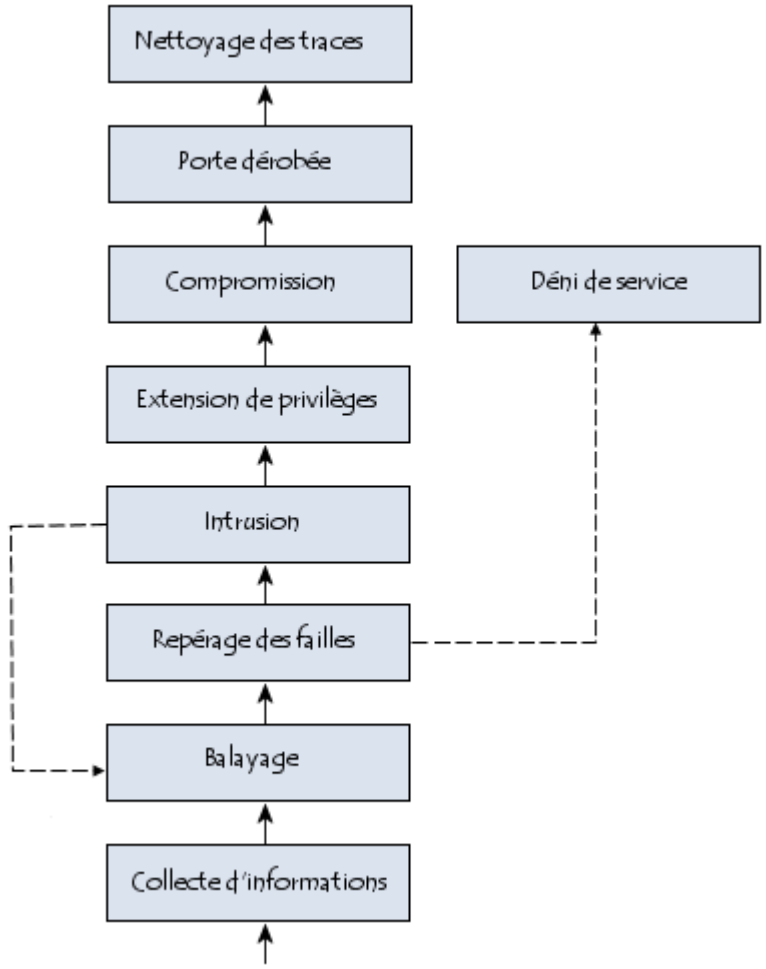


Figure 7 : Méthodologie d'une intrusion

II.13.2. La récupération d'informations sur le système :

L'obtention d'informations sur l'adressage du réseau visé, généralement qualifiée de **prise d'empreinte**, est un préalable à toute attaque. Elle consiste à rassembler le maximum d'informations concernant les infrastructures de communication du réseau cible :

- Adressage IP,
- Noms de domaine,
- Protocoles de réseau,
- Services activés,
- Architecture des serveurs,
- etc.

➢ **Consultation de bases publiques :**

En connaissant l'adresse IP publique d'une des machines du réseau ou bien tout simplement le nom de domaine de l'organisation, un pirate est potentiellement capable de connaître l'adressage du réseau tout entier, c'est-à-dire la plage d'adresses IP publiques appartenant à l'organisation visée et son découpage en sous-réseaux. Pour cela il suffit de consulter les bases publiques d'attribution des adresses IP et des noms de domaine :

- http://www.iana.net
- http://www.ripe.net pour l'Europe
- http://www.arin.net pour les Etats-Unis

➢ **Consultation de moteurs de recherche**

La simple consultation des moteurs de recherche permet parfois de glâner des informations sur la structure d'une entreprise, le nom de ses principaux produits, voire le nom de certains personnels.

II.13.3. Balayage du réseau :

Lorsque la topologie du réseau est connue par le pirate, il peut le scanner (le terme *balayer* est également utilisé), c'est-à-dire déterminer à l'aide d'un outil logiciel (appelé *scanner* ou *scanneur* en français) quelles sont les adresses IP actives sur le réseau, les ports ouverts correspondant à des services accessibles, et le système d'exploitation utilisé par ces serveurs.

L'un des outils les plus connus pour scanner un réseau est Nmap, reconnu par de nombreux administrateurs réseaux comme un outil indispensable à la sécurisation d'un réseau. Cet outil agit en envoyant des paquets TCP et/ou UDP à un ensemble de machines sur un réseau (déterminé par une adresse réseau et un masque), puis il analyse les réponses. Selon l'allure des paquets TCP reçus, il lui est possible de déterminer le système d'exploitation distant pour chaque machine scannée. [1]

Il existe un autre type de scanneur, appelé **mappeur passif** (l'un des plus connus est Siphon), permettant de connaître la topologie réseau du brin physique sur lequel le mappeur analyse les paquets. Contrairement aux scanners précédents, cet outil n'envoie pas de paquets sur le réseau et est donc totalement indétectable par les systèmes de détection d'intrusion.

Enfin, certains outils permettent de capturer les connexions X (un serveur X est un serveur gérant l'affichage des machines de type UNIX). Ce système a pour caractéristique de pouvoir utiliser l'affichage des stations présentes sur le réseau, afin d'étudier ce qui est affiché sur les écrans et éventuellement d'intercepter les touches saisies par les utilisateurs des machines vulnérables.

➢ **Lecture de bannières :**

Lorsque le balayage du réseau est terminé, il suffit au pirate d'examiner le fichier journal (*log*) des outils utilisés pour connaître les adresses IP des machines connectées au réseau et les ports ouverts sur celles-ci.

Les numéros de port ouverts sur les machines peuvent lui donner des informations sur le type de service ouvert et donc l'inviter à interroger le service afin d'obtenir des informations supplémentaires sur la version du serveur dans les informations dites de « bannière ».

Ainsi, pour connaître la version d'un serveur HTTP, il suffit de se connecter au serveur Web en Telnet sur le port 80 puis de demander la page d'accueil :

GET / HTTP/1.0

Le serveur répond alors les premières lignes suivantes :

HTTP/1.1 200 OK
Date: Thu, 21 Mar 2002 18:22:57 GMT
Server: Apache/1.3.20 (Unix) Debian/GNU

Le système d'exploitation, le serveur et sa version sont alors connus. [8]

- **Ingénierie sociale :**

L'ingénierie sociale (en anglais « *Social Engineering* ») consiste à manipuler les êtres humains, c'est-à-dire d'utiliser la naïveté et la gentillesse exagérée des utilisateurs du réseau, pour obtenir des informations sur ce dernier. Ce procédé consiste à entrer en contact avec un utilisateur du réseau, en se faisant passer en général pour quelqu'un d'autre, afin d'obtenir des renseignements sur le système d'information ou éventuellement pour obtenir directement un mot de passe. De la même façon une faille de sécurité peut être créée dans le système distant en envoyant un cheval de Troie à certains utilisateurs du réseau. Il suffit qu'un des utilisateurs exécute la pièce jointe pour qu'un accès au réseau interne soit donné à l'agresseur extérieur.

C'est la raison pour laquelle la politique de sécurité doit être globale et intégrer les facteurs humains (par exemple la sensibilisation des utilisateurs aux problèmes de sécurité) car le niveau de sécurité d'un système est caractérisé par le niveau de son maillon le plus faible.

II.13.4. Le repérage des failles :

Après avoir établi l'inventaire du parc logiciel et éventuellement matériel, il reste au hacker à déterminer si des failles existent.

Il existe ainsi des scanneurs de vulnérabilité permettant aux administrateurs de soumettre leur réseau à des tests d'intrusion afin de constater si certaines applications possèdent des failles de sécurité. Les deux principaux scanneurs de failles sont :

- Nessus
- SAINT

Il est également conseillé aux administrateurs de réseaux de consulter régulièrement les sites tenant à jour une base de données des vulnérabilités :

- SecurityFocus / Vulnerabilities

Ainsi, certains organismes, en particulier les CERT (*Computer Emergency Response Team*), sont chargés de capitaliser les vulnérabilités et de fédérer les informations concernant les problèmes de sécurité.

II.13.5. L'intrusion :

Lorsque le pirate a dressé une cartographie des ressources et des machines présentes sur le réseau, il est en mesure de préparer son intrusion.

Pour pouvoir s'introduire dans le réseau, le pirate a besoin d'accéder à des comptes valides sur les machines qu'il a recensées. Pour ce faire, plusieurs méthodes sont utilisées par les pirates :

- L'ingénierie sociale, c'est-à-dire en contactant directement certains utilisateurs du réseau (par mail ou par téléphone) afin de leur soutirer des informations concernant leur identifiant de connexion et leur mot de passe. Ceci est généralement fait en se faisant passer pour l'administrateur réseau.
- La consultation de l'annuaire ou bien des services de messagerie ou de partage de fichiers, permettant de trouver des noms d'utilisateurs valides
- L'exploitation des vulnérabilités des commandes R* de Berkeley.
- Les attaques par force brute (*brute force cracking*), consistant à essayer de façon automatique différents mots de passe sur une liste de compte (par exemple l'identifiant, éventuellement suivi d'un chiffre, ou bien le mot de passe *password*, ou *passwd*, etc).

II.13.6. Extension de privilèges :

Lorsque le pirate a obtenu un ou plusieurs accès sur le réseau en se logeant sur un ou plusieurs comptes peu protégés, celui-ci va chercher à augmenter ses privilèges en obtenant l'accès *root* (en français *superutilisateur* ou superadministrateur</i>), on parle ainsi d'**extension de privilèges**.

Dès qu'un accès *root* a été obtenu sur une machine, l'attaquant a la possibilité d'examiner le réseau à la recherche d'informations supplémentaires.

Il lui est ainsi possible d'installer un sniffeur (en anglais *sniffer*), c'est-à-dire un logiciel capable d'écouter (le terme *reniffler*, ou en anglais *sniffing*, est également employé) le trafic réseau en provenance ou à destination des machines situées sur le même brin. Grâce à cette technique, le pirate peut espérer récupérer les couples *identifiants/mots de passe* lui permettant d'accéder à des comptes possédant des privilèges étendus sur d'autres machines du réseau (par exemple l'accès au compte d'un administrateur) afin d'être à même de contrôler une plus grande partie du réseau. [9]

Les serveurs NIS présents sur un réseau sont également des cibles de choix pour les pirates car ils regorgent d'informations sur le réseau et ses utilisateurs.

II.13.7. Compromission :

Grâce aux étapes précédentes, le pirate a pu dresser une cartographie complète du réseau, des machines s'y trouvant, de leurs failles et possède un accès *root* sur au moins l'une d'entre-elles. Il lui est alors possible d'étendre encore son action en exploitant les relations d'approbation existant entre les différentes machines.

Cette technique d'usurpation d'identité, appelée spoofing, permet au pirate de pénétrer des réseaux privilégiés auxquels la machine compromise a accès.

II.13.8. Porte dérobée :

Lorsqu'un pirate a réussi à infiltrer un réseau d'entreprise et à compromettre une machine, il peut arriver qu'il souhaite pouvoir revenir. Pour ce faire celui-ci va installer une application

afin de créer artificiellement une faille de sécurité, on parle alors de **porte dérobée** (en anglais **backdoor**, le terme *trappe* est parfois également employé).

II.13.9. Nettoyage des traces :

Lorsque l'intrus a obtenu un niveau de maîtrise suffisant sur le réseau, il lui reste à effacer les traces de son passage en supprimant les fichiers qu'il a créés et en nettoyant les fichiers de logs des machines dans lesquelles il s'est introduit, c'est-à-dire en supprimant les lignes d'activité concernant ses actions.

Par ailleurs, il existe des logiciels, appelés « **kits racine** » (en anglais « *rootkits* ») permettant de remplacer les outils d'administration du système par des versions modifiées afin de masquer la présence du pirate sur le système. En effet, si l'administrateur se connecte en même temps que le pirate, il est susceptible de remarquer les services que le pirate a lancé ou tout simplement qu'une autre personne que lui est connectée simultanément. L'objectif d'un rootkit est donc de tromper l'administrateur en lui masquant la réalité.

II.14. Conclusion :

Il revient à tout responsable de réseau d'en assurer sa sécurité, et par conséquent d'en tester les failles.

C'est la raison pour laquelle, un administrateur réseau se doit d'être au courant des vulnérabilités des logiciels qu'il utilise et de se « mettre dans la peau d'un pirate » afin d'essayer de s'introduire dans son propre système et afin d'être continuellement dans un contexte de paranoïa.

La sécurisation d'un système informatique est généralement dite « asymétrique », dans la mesure où le pirate n'a qu'à trouver une seule vulnérabilité pour compromette le système, tandis que l'administrateur se doit de corriger toutes les failles.

Dans ce chapitre nous avons vu les moyens multiples à disposition de l'ennemi.

Nous allons, dans le prochain chapitre, étudier les différents mécanismes et moyens de sécurité afin de faire face aux dangers causés par les attaquants et protéger notre système d'information.

Chapitre III : Moyens technique de la sécurité

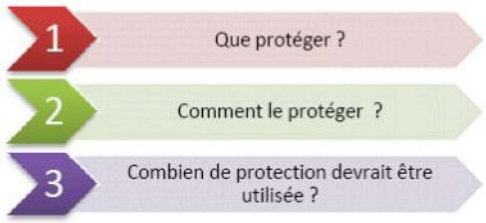
III.1. Introduction :

La tâche la plus difficile quand on traite la sécurité ou bien quand on définit la **politique de sécurité** que l'entreprise doit suivre, est probablement la phase de planification dans laquelle on développe une solution pour répondre aux besoins en sécurité et les objectifs de notre entreprise. En examinant le réseau et en identifiant les zones et les composants critiques et à risque, on devrait prendre une approche, pour créer un plan de sécurité, avec diverse objectifs en perspectives :

• Une politique de sécurité cohérente et simple devrait être créée, basée sur la stratégie et les objectifs de l'entreprise (*c.à.d. aider l'entreprise à atteindre ces objectifs, et non l'entraver par des procédures trop rigides qui vont gêner les utilisateurs dans leur travail et diminuer le rendement*).

• La politique de sécurité devra décider du choix des solutions et des produits de sécurité, mais pas l'inverse.

• La gestion de sécurité devrait être centralisée sous une seule plateforme, de préférence d'un même constructeur afin de faciliter le déploiement, le contrôle et le support de la solution. En général, une bonne politique de sécurité devrait aborder les questions suivantes :



III.2. Authentification :

La première étape afin de protéger les ressources d'un réseau est de pouvoir vérifier l'identité des utilisateurs. Cette vérification s'appelle authentification. L'authentification est la procédure mise en œuvre notamment pour vérifier l'identité d'une entité et s'assurer que l'identité fournie correspond à l'identité de cette entité préalablement enregistrée. *Dans la vie courante, l'authentification est réalisée par la carte d'identité nationale.* [3]

On authentifie un utilisateur en lui demandant de fournir quelque chose que seule cette personne a (par exemple *un jeton*), une information qu'elle seule connaît (*un mot de passe*) ou encore quelque chose qui est propre à cet utilisateur, comme une *empreinte digitale*. Plus l'utilisateur doit fournir des renseignements de ce type, plus faibles sont les risques qu'une autre personne parvienne à se faire passer pour cet utilisateur légitime. [12]

NB : Chaque politique de sécurité d'un réseau devrait exiger la mise en place d'un ou plusieurs mécanismes d'authentification.

III.2.1. Authentification forte :

En sécurité des systèmes d'information, une **authentification forte** est une procédure d'identification qui requiert la concaténation d'au moins deux facteurs d'authentification.

- **Les facteurs de l'authentification forte**

Les systèmes d'authentification courant utilisent un seul facteur (en général un mot de passe). Le principe de l'authentification forte est d'utiliser plusieurs facteurs de nature distincte afin de rendre la tâche plus compliquée à un éventuel attaquant. Les facteurs d'authentification sont classiquement présentés comme suit :

- Ce que l'entité connaît (un mot de passe, un code NIP, une phrase secrète, etc.)
- Ce que l'entité détient (une carte magnétique, RFID, une clé USB, un PDA, une carte à puce, un Smartphone, etc.). Soit un élément physique appelé authentifieur ou Token (par les anglophones)
- Ce que l'entité est, soit une personne physique (empreinte digitale, empreinte rétinienne, structure de la main, structure osseuse du visage ou tout autre élément biométrique)
- Ce que l'entité sait faire ou fait, soit une personne physique (biométrie comportementale tel que signature manuscrite, reconnaissance de la voix, un type de calcul connu de lui seul, un comportement, etc.)
- Où l'entité est, soit un endroit d'où, suite à une identification et authentification réussie, elle est autorisée (accéder à un système logique d'un endroit prescrit)

Dans la majorité des cas, l'entité est une personne physique - individu - personne morale, mais elle peut être un objet comme, par exemple, une application web utilisant le protocole SSL, un serveur SSH, un objet de luxe, une marchandise, un animal, etc. [A4]

On peut considérer que l'authentification forte est une des fondations essentielles pour garantir :

- L'autorisation ou contrôle d'accès (qui peut y avoir accès)
- La confidentialité (qui peut le voir)
- L'intégrité (qui peut le modifier)
- La traçabilité (qui l'a fait)

- **Pourquoi l'authentification forte et l'authentification à deux-facteurs?**

Le mot de passe est actuellement le système le plus couramment utilisé pour authentifier un utilisateur. Il n’offre plus le niveau de sécurité requis pour assurer la protection de biens informatiques sensibles, car différentes techniques d’attaque permettent de le trouver facilement [1]. On recense plusieurs catégories d’attaques informatiques pour obtenir un mot de passe :

- Attaque par force brute
- Attaque par dictionnaire
- Écoute du clavier informatique (*keylogger*), par voie logicielle (cheval de Troie,...), ou par écoute distante (champ électrique des claviers filaires, ou ondes radio faiblement chiffrées pour les claviers sans fils)
- Écoute du réseau (*password sniffer*) : plus facilement avec les protocole réseau sans chiffrement, comme HTTP, Telnet, FTP, LDAP, etc.

- Hameçonnage (ou filoutage), appelé en anglais *phishing*
- Attaque de l'homme du milieu ou *man in the middle attack* (MITM) : par exemple avec les protocoles SSL ou SSH
- Ingénierie sociale
- Extorsion d'informations par torture, chantage ou menaces

➢ **Familles technologiques pour l'authentification forte**

On dénombre actuellement trois familles :

- One Time Password (OTP) / Mot de passe à usage unique.
- Certificat numérique
- Biométrie

✓ ***One Time Password (OTP) / Mot de passe à usage unique***

Cette technologie permet de s'authentifier avec un mot de passe à usage unique. Elle est fondée sur l'utilisation d'un secret partagé (cryptographie symétrique) ou l'utilisation d'une carte matricielle d'authentification. Il n'est donc pas possible de garantir une véritable non-répudiation. [A4]

✓ **Certificat Numérique**

Cette technologie est fondée sur l'utilisation de la cryptographie asymétrique et l'utilisation d'un challenge. Il est possible de garantir la non-répudiation car uniquement l'identité possède la clé privée.

- Infrastructure à clés publiques (PKI)
- RSA
- PKINIT Smart Card Logon pour un environnement Microsoft

✓ **Biométrie**

Cette technologie est fondée sur la reconnaissance d'une caractéristique ou d'un comportement unique.

- Biométrie
- Technologie *Match on Card*

➢ **Authentifieur de type One-Time-Password :**

Cette technologie est fondée sur un secret partagé unique. L'authentifieur contient le secret. Le serveur d'authentification contient le même secret. Grâce au partage de ce dénominateur commun il est alors possible de générer des mots de passe à usage unique (One-Time-Password) [12]. Du fait que ce type de technologie utilise un secret partagé il n'est pas possible d'assurer la non-répudiation. La technologie du certificat numérique permet a contrario de garantir la non-répudiation.

✓ **Authentifieur fondé sur le temps :**

Ces authentifieurs utilisent, en plus du secret partagé, un dénominateur commun qui est le temps. Chaque partie est synchronisée sur le temps universel (UTC). On utilise alors un Code NIP comme deuxième facteur d'authentification [12]. Ces authentifieurs sont définis comme une technologie dite synchrone. Chaque minute, par exemple, ces authentifieurs affichent un nouveau « Token Code », le One Time Password.

L'exemple le plus connu est SecurID de la société RSA Security.

- ✓ **Authentifieur fondé sur un compteur**

Ces authentifieurs utilisent, en plus du secret partagé, un dénominateur commun qui est un compteur. Chaque partie se synchronise sur le compteur. On utilise alors un Code NIP comme deuxième facteur d'authentification [3]. Le code NIP peut être entré sur un mini clavier. Comme la technologie fondée sur le temps, ces authentifieurs ne sont pas capables d'offrir la non-répudiation. Ces authentifieurs sont définis comme une technologie dite synchrone.

- ✓ **Authentifieur fondé sur un mécanisme de « défi réponse »**

Les authentifieurs « défi-réponse » utilisent, en plus du secret partagé, un nombre aléatoire généré par le serveur d'authentification. Le client reçoit ce défi ou nonce et répond à celui-ci au serveur. On utilise alors un Code NIP comme deuxième facteur d'authentification. Le code NIP peut être entré sur un mini clavier [12]. Comme cette technologie utilise un secret partagé, ces authentifieurs ne sont pas capables d'offrir la non-répudiation.

III.2.2 Défense contre l'attaque par force brute :

- ➢ **Utilisation de mots de passe robustes**

La première défense consiste à renforcer le mot de passe en évitant les écueils qu'exploitent les attaques par force brute optimisée. Renforcer la force brute du mot de passe :

- d'allonger le mot de passe ou la clé si cela est possible ;
- utiliser la plus grande gamme de symboles possibles (minuscules, majuscules, ponctuations, chiffres) ; l'introduction de caractères nationaux (Â, ÿ…) rend plus difficile le travail des pirates (mais parfois aussi l'entrée de son mot de passe quand on se trouve à l'étranger) ;

- ➢ **Randomisation des mots de passe**

Éviter toutes les formes ou habitudes (patterns) identifiées ou identifiables par les attaquants

- éviter l'emploi de mot du langage commun pour empêcher les attaques par dictionnaire
- éviter les répétions de formes de mot de passe (par exemple les mots de passe constitué de caractères en majuscules, caractères en minuscule puis terminés par des symboles sont une famille identifiée et testée en priorité par les logiciels d'attaque par force brute)
- en poussant le raisonnement précédent jusqu'au bout il apparait que la seule méthode de choix de mot de passe qui échappe à toute optimisation est la génération aléatoire (ou en pratique une génération pseudo-aléatoire de qualité suffisante);

- **Limitation temporelle des connexions :**

La principale méthode pour neutraliser la puissance de calcul d'un attaquant consiste à limiter les tentatives possibles dans le temps. La méthode la plus restrictive et la plus sûre consiste à n'autoriser qu'un nombre limité d'erreurs avant verrouillage du système. Des méthodes moins contraignantes peuvent être de limiter le nombre de tentatives par unité de temps [1]. Ces méthodes présentent cependant des contraintes d'exploitation et peuvent être détournées par un attaquant pour créer des attaques par déni de service.

Deux brevets principaux existent à ce sujet :

- Un des Laboratoires Bell consistant à doubler le temps d'attente après chaque essai infructueux, pour le faire redescendre ensuite en vol plané après un certain temps sans attaques ;
- Un de la compagnie IBM consistant à répondre « Mot de passe invalide » après N essais infructueux en un temps T, *y compris si le mot de passe est valide* : le pirate a alors toutes les chances de rayer de façon erronée le mot de passe valide en le considérant invalide. De plus, cette méthode empêche toute attaque visant à un déni de service pour l'utilisateur.

- **Augmentation du coût par tentative :**

Une variante de l'attaque de la limitation temporelle du nombre de tentatives consiste à augmenter les ressources nécessaires pour réaliser chaque tentative.
Une première méthode consiste à utiliser une fonction de hachage cryptographique de complexité relativement élevée. Ainsi le coût de chaque tentative se trouve augmenté. Comparé à la simple temporisation, l'intérêt de l'augmentation du coût du hachage est qu'il ne peut être contourné (l'opération de hachage est strictement nécessaire pour effectuer une tentative). Les inconvénients est que le temps de l'opération baisse avec la puissance de la machine attaquante, là où la temporisation reste constante et peut être choisie de façon arbitraire, et que l'augmentation de coût s'applique également aux opérations légitimes.

Un autre exemple de système de limitation des tentatives de connexion est l'utilisation de CAPTCHA. Ces dispositifs peuvent poser des difficultés significatives pour une machine tout en restant acceptables pour un utilisateur humain.

- **Renouvellement des mots de passe**

Une solution peut constituer à limiter la durée de validité des mots de passe à une durée inférieure à celle estimée pour leur cassage en les renouvelant à intervalles réguliers. Ceci peut passer soit par une politique de sécurité informatique appliquée avec rigueur pour des périodes de renouvellement jusqu'à quelques jours ou par des dispositifs physiques *token* pour des fréquences de renouvellement très élevées.

- **Salage**

Les systèmes de mots de passe comme celui d'Unix utilisent une version modifiée du chiffrement DES. Chaque mot de passe est accompagné d'une composante aléatoire appelée *sel* dont le but est de modifier la structure interne de DES et éviter ainsi une recherche exhaustive en utilisant du matériel spécialement conçu pour DES. Ce système peut cependant

créer une faille de sécurité en facilitant les attaques par déni de service: le temps d'attente peut être utilisé pour gêner la connexion d'utilisateurs légitimes. [12]

III.3. Cryptographie :

Les récents développement de la cryptographie permettent de résoudre les nombreux problèmes menaçants la vie privé ou la sécurité sur internet, la cryptographie est l'étude des principes, méthodes et techniques mathématiques reliées aux aspects de sécurité de l'information telle la confidentialité, l'intégralité des données, authentification d'entités, et l'authentification de l'originalité des données [12]. C'est un ensemble de techniques qui fournit la sécurité de l'information. La cryptographie vous permet de stocker des informations sensibles ou de les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne peuvent être lues par personne à l'exception du destinataire convenu.

- **Les concepts généraux de la cryptographie :**

La cryptographie repose sur quatre concepts généraux : le texte en claire, l'algorithme cryptographique, le texte codé et la clé.
***Le texte en claire* :** est le message sous sa forme originale, que se soit avant le chiffrement ou après le déchiffrement.
***L'algorithme Cryptographique* :** est l'opération mathématique utilisé pour chiffrer ou déchiffrer le message.
***Le texte codé* :** est le message après qu'il a été chiffré. Le message du texte codé apparait confus et intangible aux personnes auxquels il n'est pas destiné.
***La clé* :** est un ensemble unique de caractère (tel qu'un nombre ou un mot de passe) que le chiffre utilise pour chiffrer et déchiffrer le message.

- **La cryptographie permet d'assurer :**

III.3.1. La con identialité :

La confidentialité est le premier problème posé à la cryptographie, il se résout par la notion de chiffrement.

III.3.1.1. Chiffrement :

Pour crypter un message ou un texte qu'on appellera ***texte en clair***, on lui applique une série d'opérations simples telles que la substitution et la permutation suivant des règles bien définies qui ne sont connues que par l'émetteur et le récepteur du message dans le but de le rendre inintelligible pour les tiers non autorisés (**cryptogramme** ou **texte chiffré**) et on appelle ce procédé ***chiffrement***.
Inversement, le **déchiffrement** est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans le monde de l'informatique moderne, les transformations en question sont des algorithmes construits à base de fonctions mathématiques qui dépendent d'un paramètre qu'on appelle clé de chiffrement/déchiffrement. [12]
Clé : Ensemble des données d'entrée de l'algorithme qui transforme le texte clair en texte chiffrée et inversement. Il existe deux grandes familles d'algorithmes cryptographiques à base de clefs :
a. Les algorithmes à clef privée : (*Chiffrement symétrique*) :

Le chiffrement à clé privée exige que toutes les parties qui sont autorisées à lire l'information aient la même clé que celle qui est utilisée pour le chiffrement des données.

Clef de chiffrement = clé de déchiffrement

- **Comme exemple d'algorithme à clé privée, on peut citer :** *Kerberos, Data Encryption Standard, International Data Encryption Algorithmes...*

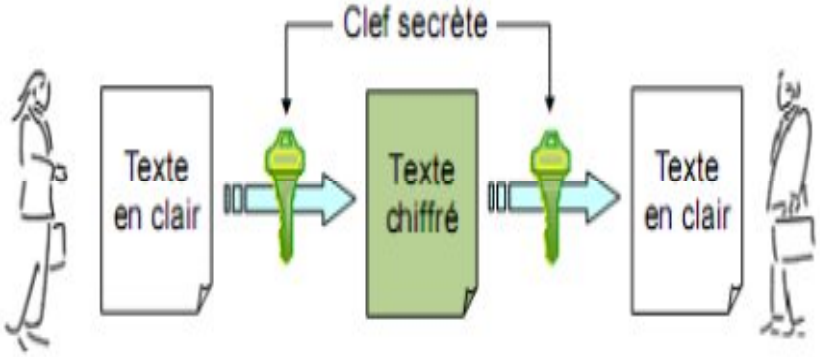


Figure 8 : Schéma représentant le chiffrement symétrique [12]

b. Les algorithmes à clef publique : (Chiffrement asymétrique) :

Clef de chiffrement ≠ clé de déchiffrement

Le chiffrement asymétrique se base sur deux clés (*une privée et une autre publique*) pour chiffrer et déchiffrer les messages. Ces clefs sont distinctes et générées en même temps et elles dépondent étroitement l'une de l'autre, c.à.d. lorsqu'on chiffre avec l'une des clés, on doit forcément déchiffrer avec l'autre. Ainsi en utilisant la clef publique, tout le monde peut chiffrer un message que seul le propriétaire de la clef privée pourra déchiffrer, et inversement, si on utilise la clef privée pour le chiffrement, tout le monde (*ceux qui possèdent la clé publique*) peut déchiffrer. [12]

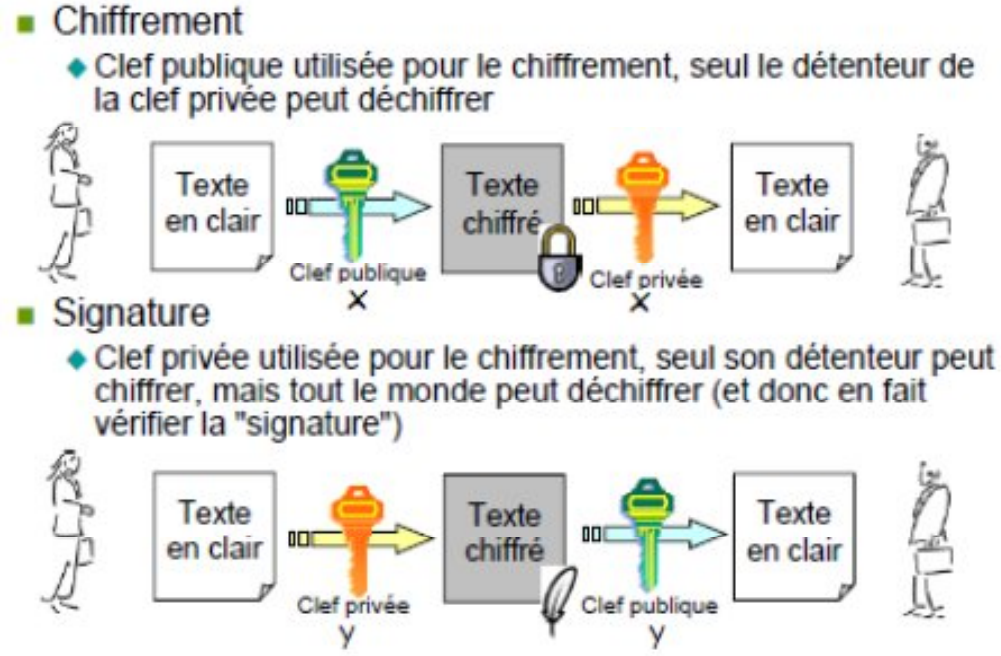


Figure 9 : Cryptographie à clef publique [12]

On peut identifier la provenance des données chiffrées par à la clef privée puisque une seule personne la possède, et donc lorsqu'une personne déchiffre le message avec sa clé publique, elle sait très bien d'où le message provient.

III.2.2. Intégrité et authenticité :

Authenticité=Authentification + Intégrité

Souvent on utilise le terme authentification afin de désigner l'authenticité, mais notez bien que l'authentification et l'intégrité sont inséparables. Lorsqu'un échange d'informations se présente au travers d'un canal de communication peu sûr, le destinataire aimerait bien s'assurer que le message s'émane de l'auteur auquel il est attribué et qu'il n'a pas été altéré pendant son voyage à travers le canal.

- **Authentification :** Consiste à s'assurer que les données s'émanent bien de l'expéditeur et non pas d'un autre utilisateur ou autre personne qui se prend pour l'expéditeur même.
- **Intégrité :** Consiste à s'assurer que les données n'ont pas été modifiées durant leur transfert. Pour répondre à ces deux critères, les signatures et les certificats numériques sont apparus.

III.3.2.1. Signature numérique:

Un des avantages majeurs de la cryptographie à clé publique est qu'elle procure une méthode permettant d'utiliser des signatures numériques. Les signatures numériques permettent à la personne qui reçoit une information de contrôler l'authenticité de son origine, et également de vérifier que l'information en question est intacte [1]. Ainsi, les signatures numériques des systèmes à clé publique permettent l'authentification et le contrôle d'intégrité des données. Une signature numérique procure également la non-répudiation, ce qui signifie qu'elle empêche l'expéditeur de contester ultérieurement qu'il ait bien émis cette information. Ces éléments sont au moins aussi importants que le chiffrement des données, sinon davantage. Une signature numérique a le même objet qu'une signature manuelle. Toutefois, une signature manuelle est facile à contrefaire. Une signature numérique est supérieure à une signature manuelle en ce qu'elle est pratiquement impossible à contrefaire et, de plus, elle atteste le contenu de l'information autant que l'identité du signataire.
La norme ISO 7498-2 définit la signature numérique comme étant des données rajoutées à une unité de données ou une transformation cryptographique d'une unité de données permettant à un destinataire de prouver la source et l'intégrité de l'unité de données en question (seul l'expéditeur est apte à générer la signature).
Sur le plan conceptuel, il est recommandé d'utiliser une clef privée car seul son possesseur pourra générer la signature et toute personne possédant la clef publique correspondante est apte de la vérifier.
La **signature numérique** est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité, par analogie avec la signature manuscrite d'un document papier. Un mécanisme de signature numérique doit présenter les propriétés suivantes :

- Il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature.
- Il doit garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

Pour cela, les conditions suivantes doivent être réunies :

- **Authentique** : L'identité du signataire doit pouvoir être retrouvée de manière certaine.
- **Infalsifiable** : La signature ne peut pas être falsifiée. Quelqu'un d'autre ne peut se faire passer pour un autre.
- **Non réutilisable**: La signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document.
- **Inaltérable** : Un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier.
- **Irrévocable** : La personne qui a signé ne peut le nier.

La signature électronique n'est devenue possible qu'avec la cryptographie asymétrique.

Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de nombres.

III.3.2.2. Fonction de hachage :

Lors d'échanges de messages chiffrés, il est important de pouvoir s'assurer que le message n'a pas été altéré ou modifié par un tiers pendant l'envoi. Les fonctions de hachage permettent alors de s'assurer de l'intégrité du message. Aussi appelée fonction de condensation, une fonction de hachage est une fonction qui convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe, la chaîne résultante est appelée ***empreinte*** (*digest* en anglais) ou condensé de la chaîne initial [3]. La fonction de hachage est une fonction à sens unique, c'est-à-dire qu'elle doit permettre de trouver facilement l'empreinte à partir du message, et d'empêcher de retrouver le message à partir de l'empreinte. Elle doit aussi être très sensible, pour qu'une petite modification du message entraîne une grande modification de l'empreinte [12]. Autre caractéristique d'une fonction de hachage, est qu'elle doit être sans collision, c'est-à-dire qu'il est impossible de trouver deux messages ayant la même empreinte. En envoyant le message accompagné de son empreinte, le destinataire peut ainsi s'assurer de l'intégrité du message en recalculant le résumé à l'arrivée et en le comparant à celui reçu. Si les deux résumés sont différents, cela signifie que le message n'est plus le même que l'original, et qu'il a été altéré ou modifié.
Exemple : MD5 (Message Digest 5) qui fournie une empreinte de 128 bits.
SHA (Secure Hash Algorithm) qui donne une empreinte de 160 bits.
NB : *On utilise souvent le terme fonction de hachage pour désigner fonction de hachage à sens unique sans collisions.*

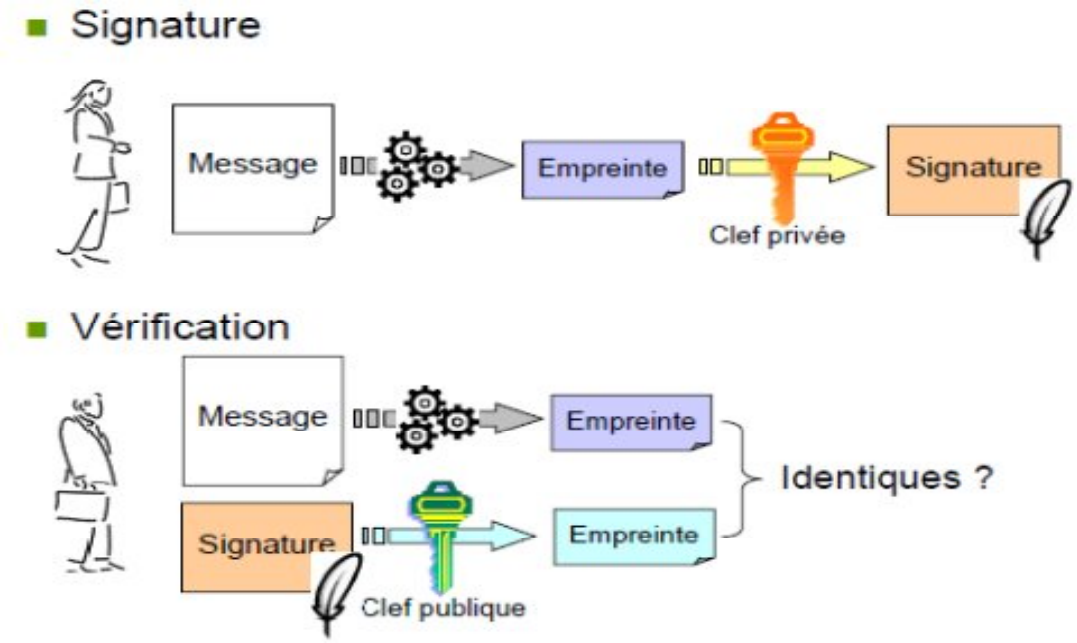


Figure 10 : Exemple de méthode de signature numérique. [12]

III.3.2.3. Certificat électronique :

Dans un environnement de clé publique, il est essentiel de s'assurer que la clé publique avec laquelle vous chiffrer les données est celle du destinataire concerné et non une contrefaçon.
Un certificat numérique ou électronique fonctionne en gros comme une pièce d'identité matérielle. Un certificat numérique est une information attachée à une clé publique, et qui permet de vérifier que cette clé est authentique, ou valide. Les certificats numériques sont utilisés pour contrecarrer les tentatives de substituer une clé falsifiée à la clé véritable. [3]
Un certificat numérique comporte trois éléments:
• Une clé publique.
• Une information de certification ('l'identité' de l'utilisateur, comme son nom, son adresse e-mail, etc.).
• Une ou plusieurs signatures numériques.
L'objet de la signature numérique sur un certificat est de garantir que les informations de certification ont été contrôlées par une autre personne ou organisme. La signature numérique ne garantit pas l'authenticité du certificat complet, elle garantit seulement que les informations d'identité ainsi signées correspondent bien à la clé publique à laquelle elles sont attachées.

III.4. VPN :

Un **réseau privé virtuel** (*Virtual Private Network* en anglais, abrégé en **VPN**) est une abstraction permettant de considérer plusieurs ordinateurs distants comme étant sur le même réseau local. Toute la partie de routage pour atteindre le ou les autres ordinateurs est gérée de façon transparente par le logiciel de VPN, créant un tunnel [13]. Cela permet ainsi de passer au travers d'un proxy, ou de se connecter au réseau local de son entreprise comme si l'on était

physiquement présent. Pour des raisons de sécurité, on ajoute généralement une couche de chiffrement au VPN.

Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole de « tunnelisation » (en anglais *tunneling*), c'est-à-dire encapsulant les données à transmettre de façon chiffrée [15]. On parle alors de VPN pour désigner le réseau ainsi artificiellement créé. Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent accéder aux données en clair.

Le VPN permet donc d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux. En contrepartie, il ne permet pas d'assurer une qualité de service comparable à une ligne spécialisée dans la mesure où le réseau physique est public, donc non garanti.

Le VPN vise à apporter certains éléments essentiels dans la transmission de données : l'authentification (et donc l'identification) des interlocuteurs, la confidentialité des données (le chiffrement vise à les rendre inutilisables par quelqu'un d'autre que le destinataire). [A5]

Cette technologie est très largement utilisée dans les entreprises d'aujourd'hui.

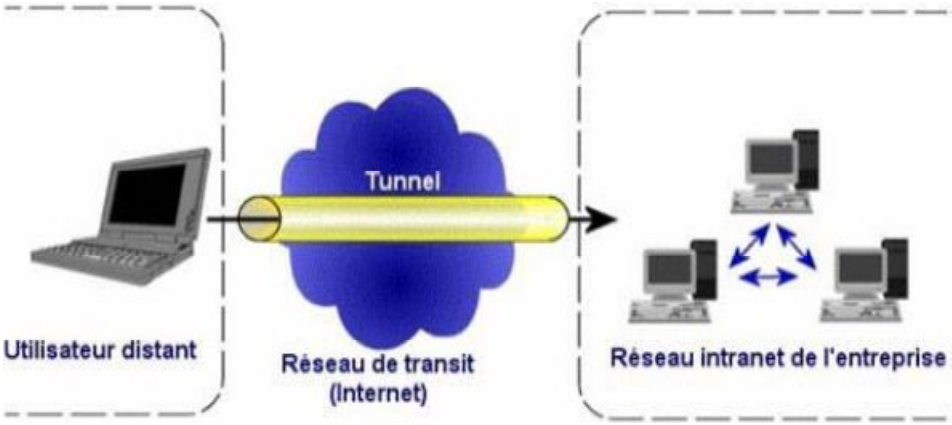


Figure 11 : Les VPN (Virtual Privat Network) : [13]

On distingue principalement deux modes d'utilisation de ces technologies :
- Le mode LAN-to-LAN permet de relier deux sites distants, par un tunnel que l'on pourrait qualifier de « permanent » entre les routeurs d'entrée des deux sites.
- Le mode End-to-LAN (ou RoadWarrior) permet à un hôte mobile d'accéder aux ressources de son entreprise de la même manière que s'il était sur site. [15]

- **VPNs LAN-to-LAN :** Il existe deux catégories de ce type:

Intranet VPN : Ce type de VPN lie plusieurs réseaux internes d une même entreprise (par exemple les réseaux de plusieurs filiales). Sans VPN, les entreprises seraient forcées d'utiliser des lignes dédiées (lignes louées) entre leurs filiales ; procédé très onéreux, surtout lorsqu' il s'agit de lignes internationales. Avec les VPN, ces mêmes communications peuvent passer

par l'Internet sans souci de confidentialité ou d'intégrité des transferts, et ce, pour un coût bien moindre. La confidentialité est basée sur les algorithmes de cryptographie. Généralement pour la confidentialité, le codage en lui-même pourra être un moyen faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable. [A5]

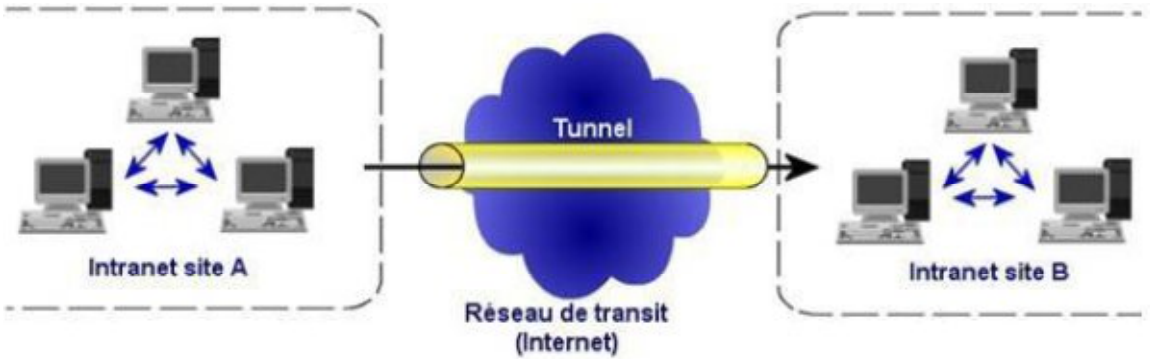


Figure 12 : Intranet VPN [13]

Extranet VPN : Cette catégorie de VPN est utilisée pour permettre aux clients, fournisseurs, partenaires ou autres interlocuteurs d'accéder à certaines données d'une entreprise. Presque tous les sites « e-commerce » ainsi que les banques, offrent ce type de connexion sécurisée à leurs clients. [A5]

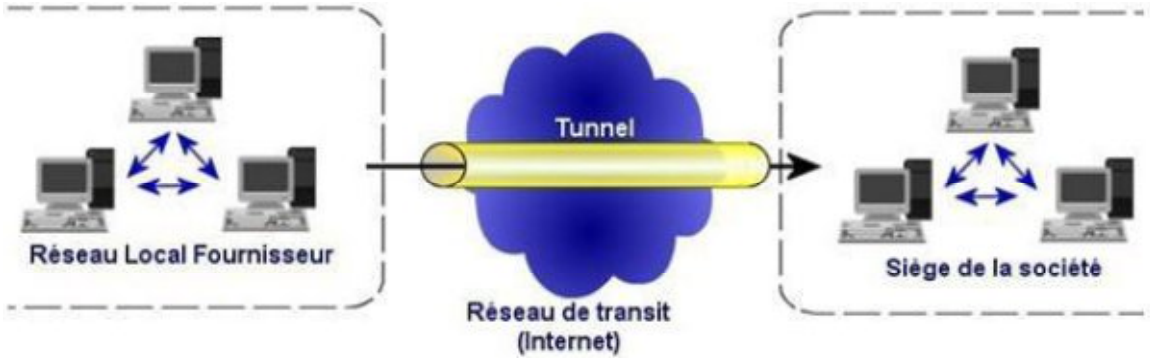


Figure 13 : Extranet VPN

- ***Caractéristiques fondamentales d'un VPN :***

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :

Authentification d'utilisateur : Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.

Gestion d'adresses : Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pourvoir se connecter facilement au réseau et recevoir une adresse.

Cryptage des données : Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
Gestion de clés : Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
Prise en charge multi protocole : La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

- **Fonctionnement :**

Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

Le terme tunnel est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées et donc normalement incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. De plus, créer un tunnel signifie aussi encapsuler un protocole dans un protocole de même niveau du modèle OSI (IP dans IPsec par exemple). Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer les données à l'entrée et serveur VPN (ou plus généralement serveur d'accès distant) l'élément déchiffrant les données en sortie.

Ainsi, lorsqu'un système extérieur à un réseau privé (client nomade, agence ou travailleur à domicile) souhaite se connecter au réseau de son entreprise :

- Les paquets (qui contiennent les données) sont chiffrés par le client VPN (selon l'algorithme décidé par les deux interlocuteurs lors de l'établissement du tunnel VPN) et éventuellement signés.
- Ils sont transmis par le biais du réseau transporteur (Internet en général).
- Ils sont reçus par le serveur VPN qui les déchiffre, les traite et regarde si les vérifications requises sont correctes.

- **Protocoles de tunnelisation :**

Les principaux protocoles de tunnelisation sont :

***IPsec* :** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

- Quelques spécifications de l'IPSec
  – Authentification, confidentialité et intégrité (protection contre l'IP spoofing et le TCP session hijacking) ;
  – Confidentialité (session chiffrée pour se protéger du sniffing) ;
  – Sécurisation au niveau de la couche transport (protection L3).
  Algorithmes utilisés:
  – Authentification pas signature DSS ou RSA ;
  – Intégrité par fonction de condensation (HMAC-MD5, HMACSHA- 1, …) ;
  – Confidentialité par chiffrement DES, RC5,IDEA,CAST, Blowfish.
- Etablissement d'une connexion IPSec
  • 2 machines doivent s'accorder pour l'utilisation des algorithmes et protocoles à utiliser

• Une SA (Security Association) est établie pour chaque connexion.
• Une SA comprend:
– Un algorithme de chiffrement (DES, 3DES) ;
– Une clé de session via IKE (Internet Key Exchange) ;
– Un algorithme d'authentification (SHA1, MD5).

***SSL/TLS* :** offre une très bonne solution de tunnelisation. L'avantage de cette solution est de permettre l'utilisation d'un navigateur Web comme client VPN.

***SSH* :** initialement connu comme remplacement sécurisé de telnet, offre la possibilité de tunneliser des connexions de type TCP, permettant d'accéder ainsi de façon sûre à des services offerts sur un réseau protégé, sans créer un réseau privé virtuel au sens plein. Toutefois, depuis sa version 4.3, le logiciel OpenSSH permet de créer des tunnels entre deux interfaces réseau virtuelles au niveau 3 (routage du seul trafic IP, interfaces TUN) ou au niveau 2 (tout le trafic Ethernet, interfaces TAP). Toutefois, OpenSSH ne gère que la création de ces tunnels, la gestion (routage, adressage, pontage, etc ...), c'est-à-dire la création du VPN utilisant ces tunnels, restant à la charge de l'utilisateur.

***VPN-Q (de Winfrasoft)* :** La mise en quarantaine des connexions permet d'isoler un utilisateur authentifié et d'inspecter sa configuration pour voir s'il ne présente aucun risque (le cas échéant de le mettre en conformité - correctifs, antivirus, pare-feu...). Ensuite et seulement s'il est conforme, il aura accès au réseau interne de l'entreprise. L'ajout de l'inspection du poste permet de réduire considérablement le risque des attaques contre le VPN. [15]

PPTP (*Point-to-Point Tunneling Protocol*) est une extension du protocole PPP (*Point-to-Point Protocol*), soumise à l'IETF en 1996. PPTP est un protocole de tunnel de la couche 2, qui permet aux données passant d'une extrémité à l'autre du tunnel d'être sécurisées par des algorithmes de cryptographie. PPTP encapsule des trames PPP dans des datagrammes IP pour une transmission sur un réseau IP, tel qu'Internet. C'est un protocole utilisé dans la mise en place des VPN.

- **Objectifs et moyens mis en œuvre :**

SSL et TLS proposent les fonctionnalités suivantes :

- *Authentification* - Le client doit pouvoir s'assurer de l'identité du serveur. Depuis SSL 3.0, le serveur peut aussi demander au client de s'authentifier. Cette fonctionnalité est assurée par l'emploi de certificats.
- *Confidentialité* - Le client et le serveur doivent avoir l'assurance que leur conversation ne pourra pas être écoutée par un tiers. Cette fonctionnalité est assurée par un algorithme de chiffrement.
- *Identification et intégrité* - Le client et le serveur doivent pouvoir s'assurer que les messages transmis ne sont ni tronqués ni modifiés (intégrité), qu'ils proviennent bien de l'expéditeur attendu.

Ces fonctionnalités sont assurées par la signature des données.

SSL et TLS reposent donc sur la combinaison de plusieurs concepts cryptographiques, exploitant la fois le chiffrement asymétrique et le chiffrement symétrique. [A5]

SSL et TLS se veut en outre évolutif, puisque le protocole est indépendant des algorithmes de cryptage et d'authentification mis en œuvre dans une transaction. Cela lui permet de s'adapter aux besoins des utilisateurs et aux législations en vigueur [15]. Cela assure de plus une meilleure sécurité, puisque le protocole n'est pas soumis aux évolutions théoriques de la cryptographie (Si un chiffrement devient obsolète, le protocole reste exploitable en choisissant un chiffrement réputé sûr).

III.5. Sécurité par l'obscurité :

Le principe de la **sécurité par l'obscurité** (de l'anglais : « security through/by obscurity ») repose sur la non-divulgation d'information relative à la structure, au fonctionnement et à l'implémentation de l'objet ou du procédé considéré, pour en assurer la sécurité.

- **Protection contre la rétro-ingénierie**

Pour éviter que quiconque puisse retrouver le code source d'un programme à partir de la version compilée (binaire), certaines sociétés utilisent des programmes pour rendre l'analyse plus ardue [1]. Il existe différentes méthodes. On peut citer :

- obfuscation du code (voir plus bas) ;
- chiffrement du programme ;
- exécution de code distant : une partie du programme est téléchargée à chaque lancement ;
- etc.

- ***Obfuscation du code machine :***

- ajout d'instructions valides inutiles et/ou d'arguments inutiles aux fonctions (pour rendre la lecture du code plus complexe).
- ajout d'instructions invalides et un saut au-dessus de ces instructions pour dérégler les désassembleurs ne supportant pas ce genre de « protection ».
- ajout de protection anti-débogueur.
- etc.

Une société peut distribuer le code source de ses programmes en les obfuscant au préalable :

- identifiants renommés avec des noms sémantiquement muets.
- suppression de l'indentation, voire de tous les espaces non significatifs.
- suppression des commentaires.
- ajout d'instructions inutiles.
- ajout d'arguments inutiles aux fonctions.
- etc.

III.6. Séparation des privilèges :

La **séparation des privilèges** est un principe qui dicte que chaque fonctionnalité ne doit posséder que les privilèges et ressources nécessaires à son exécution, et rien de plus. Ainsi en cas de défaillance grave du système, les dommages ne peuvent pas dépasser ce qui est

autorisé par les privilèges et les ressources utilisés, ces derniers étant eux-mêmes limités par la séparation de privilège.

Le cas le plus simple à comprendre est celui d'un administrateur qui doit toujours utiliser son compte utilisateur normal lorsqu'il n'a pas besoin d'accéder à des ressources appartenant à l'utilisateur root. Lorsque l'administrateur est obligé d'utiliser le compte root, il doit en limiter le plus possible la durée afin de s'exposer le moins possible à un quelconque problème.

- **Bénéfices**

- Une meilleure stabilité du système : les privilèges étant limités, les possibilités qu'une application puisse ralentir ou provoquer un crash système sont aussi limitées.
- Une meilleure sécurité du système : l'exploitation d'une faille dans un logiciel pour prendre le contrôle de la machine est rendue plus difficile pour un attaquant.
- Une facilité de déploiement accrue : La limitation des privilèges et ressources nécessaires à un logiciel permet de l'installer plus facilement.

III.7. Système de détection d'intrusion :

Un **système de détection d'intrusion** (ou IDS : *Intrusion Detection System*) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte) [14]. Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

- **Les familles de systèmes de détection d'intrusion**

Il existe trois grandes familles distinctes d'IDS :

- Les NIDS (*Network Based Intrusion Detection System*), qui surveillent l'état de la sécurité au niveau du réseau.
- Les HIDS (*HostBased Intrusion Detection System*), qui surveillent l'état de la sécurité au niveau des hôtes.
- Les IDS hybrides, qui utilisent les NIDS et HIDS pour avoir des alertes plus pertinentes.

Les HIDS sont particulièrement efficaces pour déterminer si un hôte est contaminé et les NIDS permettent de surveiller l'ensemble d'un réseau contrairement à un HIDS qui est restreint à un hôte.

- **NIDS (IDS réseau)**

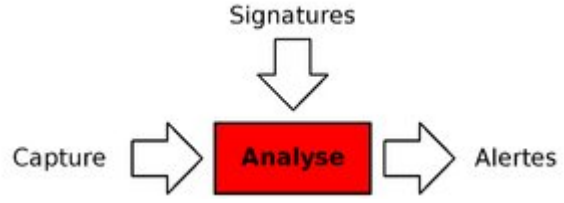


Figure 14 : Les trois parties d'un NIDS

Un NIDS se découpe en trois grandes parties : La **capture**, les **signatures** et les **alertes**.

- **Capture**

La capture sert à la récupération de trafic réseau. En général cela se fait en temps réel, bien que certains NIDS permettent l'analyse de trafic capturé précédemment.

La plupart des NIDS utilisent la bibliothèque standard de capture de paquets *libpcap*. La bibliothèque de capture de paquets *Packet Capture Library* est portée sur quasiment toutes les plates-formes, ce qui permet en général aux IDS réseau de suivre.

Le fonctionnement de la capture d'un NIDS est donc en général fortement lié à cette *libpcap*. Son mode de fonctionnement est de copier (sous Linux) tout paquet arrivant au niveau de la couche liaison de données du système d'exploitation. Une fois ce paquet copié, il lui est appliqué un filtre BPF (Berkley Packet Filter), correspondant à l'affinage de ce que l'IDS cherche à récupérer comme information.

Il se peut que certains paquets soient ignorés car sous une forte charge, le système d'exploitation ne le copiera pas.

Le comportement de la *libpcap* est différent dans le monde BSD, puisqu'il lui attache le fichier périphérique */dev/bpf*, permettant ainsi aux NIDS de ne pas avoir besoin des droits super utilisateur pour capturer le trafic mais simplement de pouvoir lire sur ce fichier sur lequel les filtres sont directement compilés. [14]

Aussi, le trafic analysé n'est pas forcément égal à celui du trafic entrant, étant donné que la *libpcap* agit à une couche en dessous du pare-feu (qui agit au niveau réseau).

- **Signatures**

Les bibliothèques de signatures (approche par scénario) rendent la démarche d'analyse similaire à celle des antivirus quand ceux-ci s'appuient sur des signatures d'attaques. Ainsi, le NIDS est efficace s'il connaît l'attaque, mais inefficace dans le cas contraire. Les outils commerciaux ou libres ont évolué pour proposer une personnalisation de la signature afin de faire face à des attaques dont on ne connaît qu'une partie des éléments. Les outils à base de signatures requièrent des mises à jour très régulières.

Les NIDS ont pour avantage d'être des systèmes temps réel et ont la possibilité de découvrir des attaques ciblant plusieurs machines à la fois. Leurs inconvénients sont le taux élevé de faux positifs qu'ils génèrent, le fait que les signatures aient toujours du retard sur les attaques de type 0day et qu'ils peuvent être la cible d'une attaque.

- **Alertes**

Les alertes sont généralement stockées dans les journaux du système. Cependant il existe une norme qui permet d'en formaliser le contenu, afin de permettre à différents éléments de sécurité d'interopérer. Ce format s'appelle IDMEF (pour *Intrusion Detection Message Exchange Format*). IDMEF est popularisé par le projet « Prélude », qui offre une infrastructure permettant aux IDS de ne pas avoir à s'occuper de l'envoi des alertes. Cela

permet aux IDS de n'avoir qu'à décrire les informations qu'il connaît et Prélude se charge de le stocker pour permettre une visualisation humaine ultérieurement.

❖ **HIDS (IDS machine)**

Les HIDS, pour Host based IDS, signifiant "Système de détection d'intrusion machine" sont des IDS dédiés à un matériel ou système d'exploitation. Généralement, contrairement à un NIDS, le HIDS récupère les informations qui lui sont données par le matériel ou le système d'exploitation. Il y a pour cela plusieurs approches : signatures, comportement (statistiques) ou délimitation du périmètre avec un système d'ACL(Access Control List). Un HIDS se comporte comme un daemon ou un service standard sur un système hôte qui détecte une activité suspecte en s'appuyant sur une norme. Si les activités s'éloignent de la norme, une alerte est générée. La machine peut être surveillée sur plusieurs points :

- Activité de la machine : nombre et listes de processus ainsi que d'utilisateurs, ressources consommées, ...
- Activité de l'utilisateur : horaires et durée des connexions, commandes utilisées, messages envoyés, programmes activés, dépassement du périmètre défini...
- Activité malicieuse d'un ver, virus ou cheval de Troie

Un autre type d'HIDS cherche les intrusions dans le « noyau » (kernel) du système, et les modifications qui y sont apportées. Certains appellent cette technique « analyse protocolaire ». Très rapide, elle ne nécessite pas de recherche dans une base de signature.

Le HIDS a pour avantage de n'avoir que peu de faux positifs, permettant d'avoir des alertes pertinentes. Quant à ses inconvénients il faut configurer un HIDS par poste et demande une configuration de chaque système.

❖ **IDS hybride**

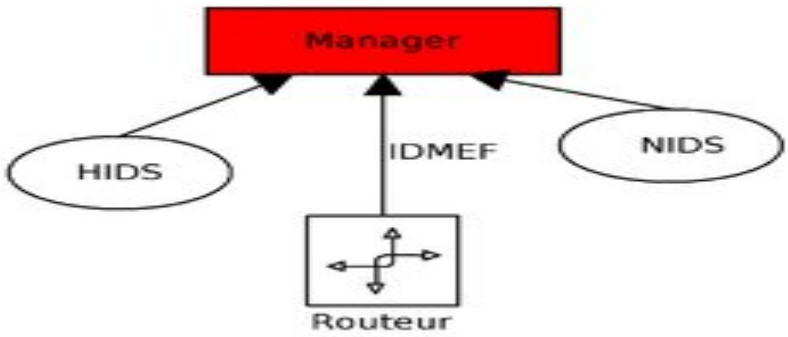


Figure 15 : Architecture d'un IDS hybride

Les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi d'alerte (typiquement IDMEF) permettant à des composants divers de communiquer et d'extraire des alertes plus pertinentes.

Les avantages des IDS hybrides sont multiples :

- Moins de faux positifs
- Meilleure corrélation

- Possibilité de réaction sur les analyseurs

➢ **Liste des IDS connus :**

- ***IDS réseau (NIDS)* :** Snort, Bro, Enterasys, Check Point, Tipping point, AIDA(Adaptive Intrusion Detection)

- ***IDS système (HIDS)* :** AIDE, Chkrootkit, DarkSpy, FCheck, IceSword, Integrit, Nabou, OSSEC, Osiris, Prelude LML, Rkhunter, Rootkit Unhooker, Samhain, Tripwire.

Ces IDS servent, entre autres, à vérifier qu'un système n'a pas été compromis (par un rootkit par exemple). Ils utilisent des sommes de contrôle (MD5, SHA-1, …) des programmes exécutables pour s'assurer qu'ils n'ont pas été modifiés.

- IDS hybride : Prelude, OSSIM.

III.8. Système de prévention d'intrusion :

Un **système de prévention d'intrusion** (ou IPS, *Intrusion Prevention System*) est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque. **C'est un IDS actif**, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement. Les IPS peuvent donc parer les attaques connues et inconnues [14]. Comme les IDS, ils ne sont pas fiables à 100 % et risquent même en cas de faux positif de bloquer du trafic légitime.

➢ **Fonctionnement des IPS :**
➢ **Types d'IPS :**

- Les HIPS (Host-based Intrusion Prevention System) qui sont des IPS permettant de surveiller le poste de travail à travers différentes techniques, ils surveillent les processus, les drivers, les .dll etc. En cas de détection de processus suspect le HIPS peut le tuer pour mettre fin à ses agissements. Les HIPS peuvent donc protéger des attaques de buffer overflow.

- Les NIPS (Network Intrusion Prevention System) sont des IPS permettant de surveiller le trafic réseau, ils peuvent prendre des mesures telles que terminer une session TCP. Une déclinaison en WIPS (Wireless Intrusion Prevention System) est parfois utilisée pour évoquer la protection des réseaux sans-fil.

- Il existe aussi les KIPS (Kernel Intrusion Prevention System) qui permettent de détecter toutes tentatives d'intrusion au niveau du noyau, mais ils sont moins utilisés.

➢ **Les techniques de détection d'intrusion :**
  ▪ **Les inconvénients de l'IPS :**

Les IPS ne sont pas des logiciels miracle qui vous permettront de surfer en toute quiétude sur le net. Voici quelques-uns de leurs inconvénients :

- Ils bloquent tout ce qui parait infectieux à leurs yeux, mais n'étant pas fiable à 100 % ils peuvent donc bloquer malencontreusement des applications ou des trafics légitimes.
- Ils laissent parfois passer certaines attaques sans les repérer, et permettent donc aux pirates d'attaquer un PC.
- Ils sont peu discrets et peuvent être découverts lors de l'attaque d'un pirate qui une fois qu'il aura découvert l'IPS s'empressera de trouver une faille dans ce dernier pour le détourner et arriver à son but.

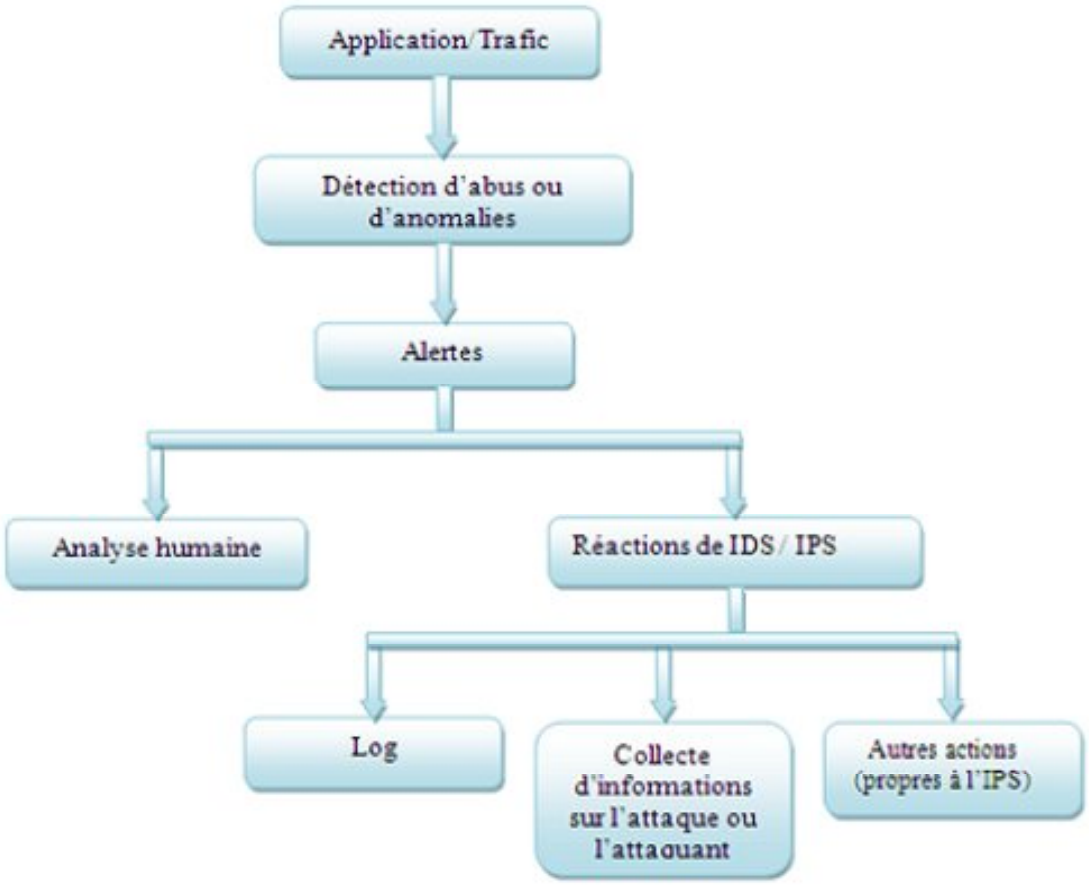


Figure 16 : Architecture et fonctionnement d'un IDS / IPS

III.9. Pot de miel :

Dans le jargon de la sécurité informatique, un **pot de miel**, ou **honeypot**, est une méthode de défense active qui consiste à attirer, sur des ressources (serveur, programme, service), des adversaires déclarés ou potentiels afin de les identifier et éventuellement de les neutraliser.

Le terme désigne à l'origine des dispositifs informatiques spécialement conçus pour susciter des attaques informatiques. Son usage s'est étendu à des techniques relevant de l'ingénierie sociale et du renseignement humain.

- **Principes de fonctionnement**

Le but de ce leurre est de faire croire à l'intrus qu'il peut prendre le contrôle d'une véritable machine de production, ce qui va permettre à l'administrateur d'observer les moyens

de compromission des attaquants, de se prémunir contre de nouvelles attaques et lui laisser ainsi plus de temps pour réagir. [1]

Une utilisation correcte d'un pot de miel repose essentiellement sur la résolution et la mise en parallèle de trois problématiques :

- la surveillance ;
- la collecte d'information ;
- l'analyse d'information.

❖ **Surveillance**

Il faut partir du principe que toute information circulant sur le réseau à destination ou non du pot de miel est importante. De ce fait, la surveillance doit absolument être constante et doit porter aussi bien au niveau local qu'au niveau distant. Cette surveillance de tous les instants repose sur :

- l'analyse du trafic réseau ;
- l'analyse pré compromission ;
- la journalisation des événements.

❖ **Collecte d'informations**

La collecte d'informations est possible grâce à des outils appelés renifleurs qui étudient les paquets présents sur le réseau et stockent les événements dans des bases de données. On peut également collecter des informations brutes grâce à des analyseurs de trames.

❖ **Analyse d'informations**

C'est grâce à l'analyse des informations recueillies que l'on va pouvoir découvrir les défaillances du réseau à protéger et les motivations des attaquants.

➢ **Différents types de pot de miel**

On compte deux types de pots de miel qui ont des buts et des fonctionnalités bien distincts :

- Les pots de miel à faible interaction ;
- Les pots de miel à forte interaction.

❖ **Pots de miel à faible interaction**

Ils sont les plus simples de la famille des pots de miel. Leur but est de recueillir un maximum d'informations tout en limitant les risques en offrant un minimum de privilèges aux attaquants.

On peut ranger, par exemple, la commande netcat dans cette catégorie. Netcat peut écouter un port particulier et enregistrer dans un journal toutes les connexions, ainsi que les commandes entrées. Ce programme permet donc d'écrire dans un fichier toutes les commandes entrées par des agresseurs. Cependant, ce type d'écoute reste très limité car il faut exécuter la commande pour chaque port que l'on souhaite observer.

Dans la même famille, on peut citer :

- *Honeyd*, de Niels Provost, qui est un pot de miel virtuel capable d'émuler des machines ou un réseau virtuel dans le but de leurrer les hackers. C'est l'un des pots de miel à faible interaction qui offre le plus de possibilités.
- *Specter*, qui permet d'émuler des services classiques (web, FTP, etc.). Il ne permet pas à l'attaquant l'accès total à un système d'exploitation, ce qui limite son intérêt.

❖ **Pots de miel à forte interaction**

Ce type de pot de miel peut être considéré comme le côté extrême du sujet puisqu'il repose sur le principe de l'accès à de véritables services sur une machine du réseau plus ou moins sécurisée.

Les risques sont beaucoup plus importants que pour les pots de miel à faible interaction. Il apparaît donc nécessaire de sécuriser au maximum l'architecture du réseau pour que l'attaquant ne puisse pas rebondir et s'en prendre à d'autres machines.

Les deux grands principes d'un tel pot de miel sont :

- le contrôle de données : pour observer le maximum d'attaques, le pot de miel à forte interaction doit accepter toutes les connexions entrantes et au contraire limiter les connexions sortantes pour éviter tout débordement. Cependant, il ne faut en aucun cas interdire toutes les connexions sortantes pour ne pas alerter l'attaquant. Un bon compromis entre sécurité et risque de découverte du leurre est donc nécessaire. [3]

- la capture des données : avec un pare-feu ou un système de détection d'intrusion (SDI).
    - le pare-feu permet de *loguer* et de rediriger toutes les tentatives d'attaque aussi bien internes qu'externes.
    - le SDI permet d'enregistrer tous les paquets circulant pour pouvoir reconstruire la séquence d'attaque. Il peut permettre également, grâce aux iptables, de rediriger les paquets compromis vers le pot de miel. Il vient donc en complément d'un pare-feu et sert également de sauvegarde au cas où celui-ci tomberait.
    - les informations générées seront redirigées vers une machine distante et non stockées sur la machine compromise en raison du risque de compromission de ces données.

Il faut également relever l'existence de pots de miel plus spécifiques comme les pots de miel anti-spam ou anti-virus.

Les honeys pot sont des systèmes employés pour leurrer des intrus en exposant des vulnérabilités connues délibérément. Une fois qu'un intrus trouve un honey pot , il est plus probable que l'intrus s'y colle pendant un certain temps. Pendant ce temps, l'administrateur pourra enregistrer les activités de l'intrus pour découvrir ses actions et ses techniques. Une fois qu'il connaît ces techniques, il peut employer ces informations plus tard pour durcir la sécurité sur des serveurs réels de l'entreprise.
Il y a différentes manières de construire et placer des honeys pot. Le honey pot devrait avoir des services communs en fonctionnement. Ces services communs incluent le serveur telnet

(port 23), le serveur HTTP (port 80), le serveur ftp (port 21) et ainsi de suite. L'administrateur devra placer le honey pot quelque part près du serveur de production de sorte que les intrus puissent facilement le prendre pour un vrai serveur. Par exemple, si les serveurs de production ont les adresses 192.168.10.21 et 192.168.10.23 du Internet Protocol (IP), l'administrateur assignera une adresse IP comme 192.168.10.22 dans le honey pot. Il peut également configurer le firewall et/ou routeur pour réorienter le trafic de quelques ports vers le honey pot où l'intrus pensera que il/elle se relie à un vrai serveur.
L'administrateur devra prendre quelques précautions comme créer un mécanisme d'alerte, de sorte que quand votre honey pot est compromis, il vous l'annonce immédiatement, et aussi, de garder des fichiers de log sur une autre machine afin que l'intrus n'ait pas la capacité de supprimer ces fichiers (lorsque le honey pot est compromis). [A8]
Dans le meilleur des cas, un honey pot devrait ressembler à un vrai système. L'administrateur doit créer de faux fichiers de données, comptes d'utilisateur... pour assurer que l'intrus s'y croit vraiment. Ceci donnera envie à l'intrus de rester sur le honey pot pendant longtemps et ainsi l'administrateur pourra enregistrer plus d'activité.

III.10. Pare-feu :

Un **pare-feu** (de l'anglais *firewall*), est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés sur ce réseau informatique. Il mesure la prévention des applications et des paquets.

- **Terminologie**

Un pare-feu est parfois appelé coupe-feu, garde-barrière, barrière de sécurité, ou encore firewall.

Dans un environnement Unix BSD (Berkeley Software Distribution), un pare-feu est aussi appelé *packet filter*. [15]

III.10.1. Fonctionnement général :

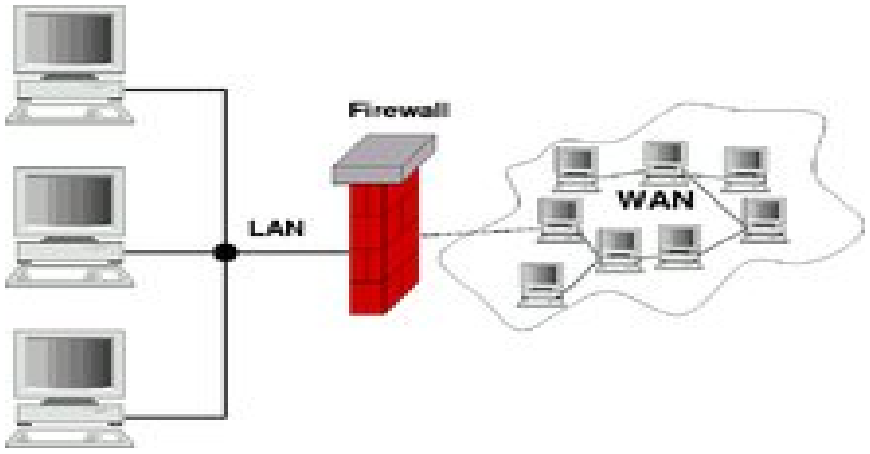


Figure 17 : Pare-feu passerelle entre LAN et WAN

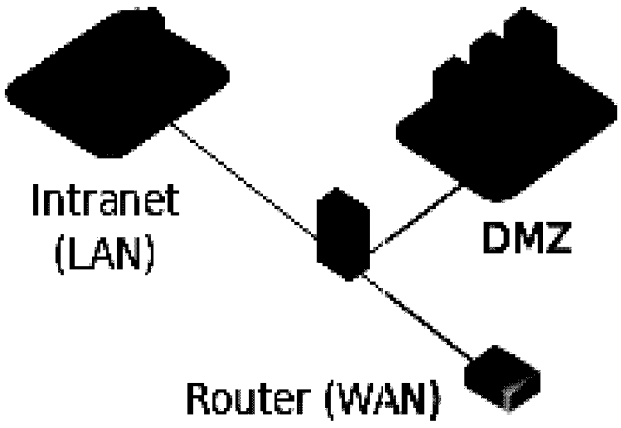


Figure 18 : Pare-feu routeur, avec une zone DMZ

Le pare-feu était jusqu'à ces dernières années considéré comme une des pierres angulaires de la sécurité d'un réseau informatique (il perd en importance au fur et à mesure que les communications basculent vers le HTTP sur SSL, court-circuitant tout filtrage). Il permet d'appliquer une politique d'accès aux ressources réseau (serveurs).

Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent. Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante).

Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège.

Le filtrage se fait selon divers critères. Les plus courants sont :

- l'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, etc.) ;
- les options contenues dans les données (fragmentation, validité, etc.) ;
- les données elles-mêmes (taille, correspondance à un motif, etc.) ;
- les utilisateurs pour les plus récents.

Un pare-feu fait souvent office de routeur et permet ainsi d'isoler le réseau en plusieurs zones de sécurité appelées zones démilitarisées ou DMZ. Ces zones sont séparées suivant le niveau de confiance qu'on leur porte.

- **Zone démilitarisée :**

Une **zone démilitarisée** (ou **DMZ**, de l'anglais *demilitarized zone*) est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet. [15]

Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ.

En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local.

La figure 20 représente une architecture DMZ avec un pare-feu à trois interfaces. L'inconvénient est que si cet unique pare-feu est compromis, plus rien n'est contrôlé. Il est cependant possible d'utiliser deux pare-feu en cascade afin d'éliminer ce risque. Il existe aussi des architectures de DMZ où celle-ci est située entre le réseau Internet et le réseau local, séparée de chacun de ces réseaux par un pare-feu.

Enfin, le pare-feu est également souvent extrémité de tunnel IPsec ou SSL. L'intégration du filtrage de flux et de la gestion du tunnel est en effet nécessaire pour pouvoir à la fois protéger le trafic en confidentialité et intégrité et filtrer ce qui passe dans le tunnel.

Les firewalls opèrent dans ces quatre couches du modèle OSI :

Figure 19 : les couches OSI utilisées par les firewalls

III.10.2. Catégories de pare-feu :

Les pare-feu sont un des plus vieux équipements de sécurité informatique et, en tant que tels, ils ont été soumis à de nombreuses évolutions. Suivant la génération du pare-feu ou son rôle précis, on peut les classer en différentes catégories.

- **Pare-feu sans état (*stateless firewall*)**

C'est le plus vieux dispositif de filtrage réseau, introduit sur les routeurs. Il regarde chaque paquet indépendamment des autres et le compare à une liste de règles préconfigurées.

La configuration de ces dispositifs est souvent complexe et l'absence de prise en compte des machines à états des protocoles réseaux ne permet pas d'obtenir une finesse du filtrage très évoluée. Ces pare-feu ont donc tendance à tomber en désuétude mais restent présents sur certains routeurs ou systèmes d'exploitation.

- **Pare-feu à états (*stateful firewall*)**

Certains protocoles dits « à états » comme TCP introduisent une notion de connexion. Les pare-feu à états vérifient la conformité des paquets à une connexion en cours. C'est-à-dire qu'ils vérifient que chaque paquet d'une connexion est bien la suite du précédent paquet et la réponse à un paquet dans l'autre sens. Ils savent aussi filtrer intelligemment les paquets ICMP qui servent à la signalisation des flux IP. [15]

Enfin, si les ACL autorisent un paquet UDP caractérisé par un quadruplet (ip_src, port_src, ip_dst, port_dst) à passer, un tel pare-feu autorisera la réponse caractérisée par un quadruplet inversé, sans avoir à écrire une ACL inverse. Ceci est fondamental pour le bon fonctionnement de tous les protocoles fondés sur l'UDP, comme DNS par exemple. Ce mécanisme apporte en fiabilité puisqu'il est plus sélectif quant à la nature du trafic autorisé. Cependant dans le cas d'UDP, cette caractéristique peut être utilisée pour établir des connexions directes (P2P) entre deux machines (comme le fait Skype par exemple).

- **Pare-feu applicatif**

Dernière mouture de pare-feu, ils vérifient la complète conformité du paquet à un protocole attendu. Par exemple, ce type de pare-feu permet de vérifier que seul du protocole HTTP passe par le port TCP 80. Ce traitement est très gourmand en temps de calcul dès que le débit devient très important. Il est justifié par le fait que de plus en plus de protocoles réseaux utilisent un tunnel TCP afin de contourner le filtrage par ports.

Une autre raison de l'inspection applicative est l'ouverture de ports dynamique. Certains protocoles comme le fameux FTP en mode passif échangent entre le client et le serveur des adresses IP ou des ports TCP/UDP. Ces protocoles sont dits « **à contenu sale** » ou « passant difficilement les pare-feu » car ils échangent au niveau applicatif (FTP) des informations du niveau IP (échange d'adresses) ou du niveau TCP (échange de ports). Ce qui transgresse le principe de la séparation des couches réseaux. Pour cette raison, les protocoles « à contenu sale » passent difficilement voire pas du tout les règles de NAT ...dynamiques, à moins qu'une inspection applicative ne soit faite sur ce protocole. [15]

Chaque type de pare-feu sait inspecter un nombre limité d'applications. Chaque application est gérée par un module différent pour pouvoir les activer ou les désactiver. La terminologie pour le concept de module est différente pour chaque type de pare-feu : par exemple : Le protocole HTTP permet d'accéder en lecture sur un serveur par une commande GET, et en écriture par une commande PUT. Un pare-feu applicatif va être en mesure d'analyser une connexion HTTP et de n'autoriser les commandes PUT qu'à un nombre restreint de machines.

- **Pare-feu identifiant**

Un pare-feu réalise l'identification des connexions passant à travers le filtre IP. L'administrateur peut ainsi définir les règles de filtrage par utilisateur et non plus par adresse IP ou adresse MAC, et ainsi suivre l'activité réseau par utilisateur.

Plusieurs méthodes différentes existent qui reposent sur des associations entre IP et utilisateurs réalisées par des moyens variés. On peut par exemple citer authpf (sous OpenBSD) qui utilise ssh pour faire l'association. Une autre méthode est l'identification connexion par connexion (sans avoir cette association IP=utilisateur et donc sans compromis sur la sécurité), réalisée par exemple par la suite NuFW, qui permet d'identifier également sur des machines multi-utilisateurs.
On pourra également citer Cyberoam qui fournit un pare-feu entièrement basé sur l'identité (en réalité en réalisant des associations adresse MAC = utilisateur) ou Check Point avec l'option NAC Blade qui permet de créer des règles dynamiques basée sur l'authentification Kerberos d'un utilisateur, l'identité de son poste ainsi que son niveau de sécurité (présence d'antivirus, de patchs particuliers). [15]

- **Pare-feu personnel**

Les pare-feu personnels, généralement installés sur une machine de travail, agissent comme un pare-feu à états. Bien souvent, ils vérifient aussi quel programme est à l'origine des données. Le but est de lutter contre les virus informatiques et les logiciels espions.

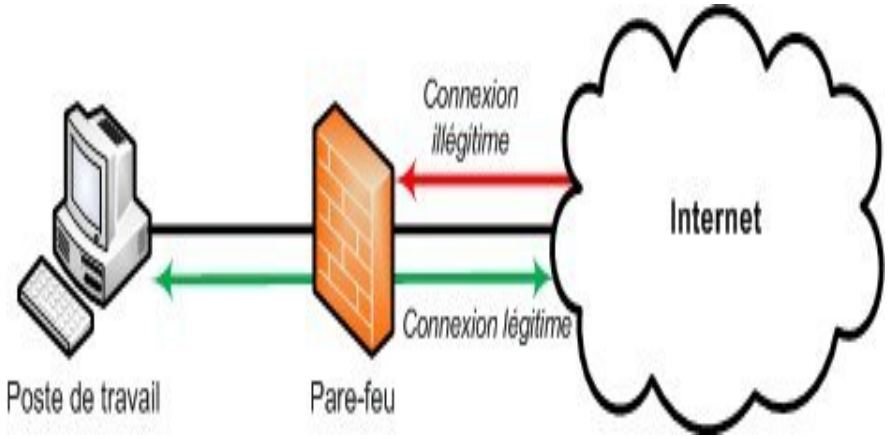


Figure 20 : pare-feu personnel

Dans le cas d'un pare-feu personnel, c'est un logiciel qui tourne sur le poste de l'internaute qui assure le filtrage.

La plupart des pare-feu personnels peuvent filtrer les applications qui tentent de se connecter à l'internet ou qui attendent une connexion de l'extérieur. L'utilisateur est en général prévenu par un message d'alerte, via lequel il peut accepter ou refuser cette connexion au cas par cas ou définitivement. Ce mode d'utilisation est aussi appelé mode d'apprentissage.

Certains pare-feu personnels vérifient également que le logiciel qui tente de se connecter sur le réseau n'a pas été altéré par un cheval de Troie.

- **Portail captif**

Les portails captifs sont des pare-feux dont le but est d'intercepter les usagers d'un réseau de consultation afin de leur présenter une page web spéciale (par exemple : avertissement, charte d'utilisation, demande d'authentification, etc.) avant de les laisser accéder à Internet. Ils sont utilisés pour assurer la traçabilité des connexions et/ou limiter l'utilisation abusive des moyens d'accès. On les déploie essentiellement dans le cadre de réseaux de consultation Internet mutualisés filaires ou Wi-Fi.

III.10.3. Technologies utilisées :

Les pare-feu récents embarquent de plus en plus de fonctionnalités, parmi lesquelles on peut citer :

- Filtrage sur adresses IP / protocole,
- Inspection *stateful*[2] et applicative,
- Intelligence artificielle pour détecter le trafic anormal,
- Filtrage applicatif :

  - HTTP (restriction des URL accessibles),
  - Courriel (Anti-pourriel),
  - Logiciel antivirus, anti-logiciel malveillant
- Traduction d'adresse réseau,
- Tunnels IPsec, PPTP, L2TP,
- Identification des connexions,
- Serveurs de protocoles de connexion (telnet, SSH), de protocoles de transfert de fichier (SCP),
- Clients de protocoles de transfert de fichier (TFTP),
- Serveur Web pour offrir une interface de configuration agréable,
- Serveur mandataire (« *proxy* » en anglais),
- Système de détection d'intrusion (« IDS » en anglais),
- Système de prévention d'intrusion (« IPS » en anglais).

➢ **Parefeu basé sur la sécurité :**

IPCop :

IPCop est une distribution Linux basée sur Linux From Scratch, qui vise à fournir un pare-feu simple à gérer basé sur du matériel PC. IPCop est un pare-feu à états construit sur le framework netfilter de Linux. [A8]

Elle vise à fournir un moyen simple mais puissant pour configurer un pare-feu sur une architecture de type PC. Elle peut protéger sur une telle architecture un réseau familial ou de petites ou moyennes entreprises, elle offre la classique Zone démilitarisée ainsi que les tunnels réseau privé virtuel (acronyme VPN en anglais).

IPCop peut également servir de serveur mandataire (proxy), serveur fournissant des adresses IP dynamique (DHCP), de relais DNS, de serveur de temps (NTP), et en installant des greffons ou modules, de bien d'autres choses (contrôle de contenu, liste noire, liste d'accès, DNS dynamique, contrôle de trafic, etc.). Le support des clients sans fil est aussi prévu par le biais d'une zone dédiée.

À l'origine, IPCop était un fork de la distribution Linux Smoothwall, depuis ces deux projets se sont développés indépendamment, et maintenant divergent de manière importante.

III.11. **Proxy :**

Il existe une autre architecture qui ne se repose pas sur l'usage d'un pare-feu, le principe consiste à déconnecter complètement le réseau local du réseau extérieur puis à mettre des passerelles nommées proxy entre les deux réseaux pour relayer les demandes du réseau interne vers le réseau extérieur.
La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, SOCKS).

➢ ***Nécessité d'un proxy dans une entreprise* :**

L'accès à l'information par l'Internet est devenu un réel besoin pour les employés de votre société, il est synonyme d'information cohérente, rapide et spécialisée permettant à chaque individu d'améliorer sa propre productivité au sein de votre organisation.
Toutefois, l'Internet propose l'accès à tous types d'informations sur tous types de sujets. Ainsi, certaines de ces informations (certains de ces sites Web) n'ont aucun intérêt pour l'activité professionnelle de vos employés.
De plus, ces informations ayant pour beaucoup d'entre elles un caractère ludique, l'accès illimité et non contrôlé à l'ensemble des sujets proposés sur l'Internet peut pousser vos utilisateurs à un usage important et complètement improductif de l'outil Internet. [10]
Tous ceci peut conduire l'entreprise a des perte de productivité importante, pour pallier à ce problème l'entreprise doit prendre des dispositions de sécurité,

- ***Le principe du fonctionnement d'un proxy*** **:**

Le principe du fonctionnement d'un serveur proxy est assez simple : par exemple si vous voulez que vos utilisateurs aient accès au Web, vous pouvez alors installer un proxy web entre votre réseau local et Internet.
Il vous faudra alors configurer le navigateur Internet de chaque utilisateur pour lui indiquer l'adresse de votre proxy.
Cette modification réalisée, lorsque l'utilisateur souhaite consulter une page web, le navigateur ne va pas s'adresser directement au site web sur Internet mais va rédiger la demande vers le proxy de l'entreprise.
C'est ensuite le proxy qui demandera la page au serveur web Internet, la rapatriera entièrement, puis la transmettra au navigateur de l'utilisateur, pour l'utilisateur le résultat sera transparent.

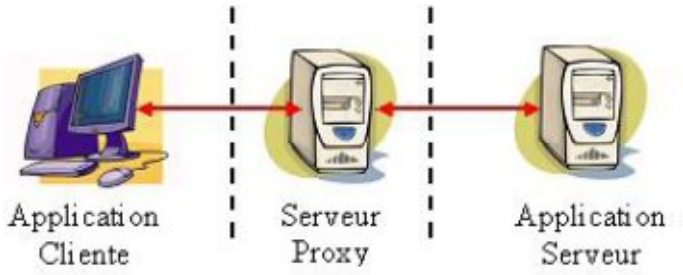


Figure 21 : Client serveur fonctionnant avec un proxy

- ***Les fonctionnalités d'un serveur proxy*** **:**

Désormais, avec l'utilisation de TCP/IP au sein des réseaux locaux, le rôle de relais du serveur proxy est directement assuré par les passerelles et les routeurs. Les serveurs proxys (mandataire) sont notamment utilisés pour assurer les fonctions suivantes :
• mémoire cache,
• Le filtrage,
• Enregistrement,
• L'authentification.

III.12.Translation d'adresse :

La translation d'adresse consiste à utiliser une seul adresse IP publique officiel qui sera attribué a votre par feu ou bien votre proxy, vous attribuez ensuite des adresse IP privées à chaque machine de votre réseau local.

Les adresse privées ne sont routées par le réseau internet, Si une machine de votre réseau local possédant une adresse privée telle que 192.168.0.0 par exemple, souhaite communiquer avec un serveur se trouvant sur internet, elle pourra le joindre, mais celui-ci ne pourra pas répondre car le paquet de retour sera détruit par les routeurs du réseau Internet. [10]
Avec la translation d'adresse le proxy ou le par feu transforme en temps réel les adresse privés en adresse publique, puis au retour de la réponse, l'adresse publique en adresse privé.
Ainsi même si vous avez plusieurs poste utilisateurs disposant chacune d'une adresse privé différente, vu de l'extérieur, c'est comme s'il n y avait qu'un seul utilisateur ans l'entreprise.

- ***Avantages en termes de sécurité de la translation d'adresse***

L'avantage d'utiliser une translation d'adresse pour votre réseau local réside dans le fait que ces adresses privées ne seront pas utilisables sur internet.
Même si votre par feu est mal réglé, un pirate qui essaierait de communiquer avec une machine utilisateur de votre réseau local ayant une adresse IP privé n'obtiendrait aucune réponse car tous les paquets qu'il enverrait serait détruit par le réseau, les paquets n'arriverai même pas jusqu'à votre par feu.
En revanche, les utilisateurs du réseau local n'auront aucun problème pour communiquer vers le réseau Internet car tous les paquets sortant seront traités par la translation d'adresse.
Par ailleurs si votre par feu ou bien votre proxy cesse de fonctionner ou bien s'arrête complètement pour une raison ou une autre, la fonction de translation d'adresse s'arrêtera en même temps, de ce fait aucune machine n'arriverait a communiquer avec l'internet.

III.13. L'analyse des journaux :

Pour permettre la sauvegarde des flux réseau entrant et sortant, il faut effectuer des opérations d'enregistrement sur fichier, des fichiers logs.
Un fichier log est un fichier sous forme ASCII (américain standard code for information and inter change). Le fichier log est porteur d'informations essentielles qui concernent toutes les activités du serveur, car ce fichier est crée en général au niveau du serveur par un logiciel. Le contenu d'un fichier log et fonction du type d'activité du serveur. Un fichier log d'un serveur du réseau par exemple doit contenir la trace du trafic des réseaux entrant et sortant durant tout le temps de son activité.
Plusieurs formats existent pour les fichiers logs, le contenu des fichiers log dépend de l'activité du serveur et du niveau d'enregistrement.
Par ailleurs, la de notation du fichier log veux dire « le journal de bord des connexions ».
C'est en quelque sorte un fichier qui sert d'historique pour administrateur réseau, et qui renferme la trace de toute les requêtes et réponse concernant le serveur sur lequel la journalisation est effectué

III.14. Durcissement :

Le **durcissement** est le processus destiné à sécuriser un système. La démarche consiste principalement à réduire à l'indispensable les objets (logiciels, bibliothèques logicielles, outils) installés sur le système, ainsi qu'à éliminer les utilisateurs et les droits non indispensables, tout en conservant les fonctionnalités requises. [1]

Le principe sous-jacent est la réduction de la surface d'attaque possible, en considérant que tout objet installé est potentiellement une source de vulnérabilité (exploit). La réduction du nombre d'objets installés réduit donc le nombre de failles possibles, pour un système donné.

III.15. Logiciels anti-malveillants :

III.15.1. Logiciel anti-espion:

Logiciel destiné à supprimer les logiciels espions installés sur votre ordinateur. *Synonymes :* antispyware, anti-espiogiciel

Logiciels anti-espions **:** Ad-Aware, ClamAV, ClamWin, Hitman pro, Malwarebytes' Anti-Malware, Moon Secure AV, afetyGate Invisible, Spybot - Search & Destroy, Spyware Doctor, Spyware terminator, SpywareBlaster, SpywareGuard, System Doctor,Windows Defender, Winpooch

- **Ad-Aware** est un logiciel de la société Lavasoft qui détecte et supprime les virus, les logiciels considérés comme des publiciels (sa vocation première) et des logiciels espion (spyware, malware). Il détecte également les composeurs, les chevaux de Troie et les autres logiciels malveillants.

III.15.2. Logiciel anti-rootkit :

Logiciel de sécurité permettant la détection et la neutralisation ou la suppression des rootkits.

Logiciels anti-rootkit **:** Chkrootkit, DarkSpy, IceSword, Rkhunter, Rootkit Unhooker, RootkitRevealer, SafetyGate Invisible, Spyware terminator

III.15.3.Logiciel anti-spam :

La lutte antipourriel est un ensemble de comportements, de systèmes et de moyens techniques et juridiques permettant de combattre le pourriel.

- ***Logiciels anti-spam*****:** Bogofilter, MIMEDefang, OutClock, PersonalAntispam, SpamAssassin, Spamd, Spamihilator, SpamPal, SpamWars

- **Bogofilter :**

Est un logiciel libre sous licence GPL(Licence Publique Générale) de classification de courrier électronique en spam si il est indésirable) ou ham dans le cas contraire, basé sur une analyse statistique de l'en-tête et du contenu du message. Le programme est capable d'apprendre à partir des classifications opérées par l'utilisateur. Ce logiciel utilise la technique statistique de filtrage bayésien pour effectuer sa classification. Sa première utilisation en matière de spam a été décrite dans l'article de Paul Graham A Plan For Spam. Gary Robinson, dans son weblog Rants, a proposé des améliorations pour rendre la discrimination entre Spam et ham plus pertinente [1]. Bogofilter est appelé par un script du MDA, après la partie de vérification de validité de l'émetteur dans la chaine des filtres anti-spam, afin de classer un message entrant en spam ou ham en se basant sur des dictionnaires stockés dans une base Berkeley DB, SQLite3 ou encore QDBM). Bogofilter est aussi à l'aise sur du texte brut que sur du HTML. Il supporte également les messages au format MIME. En revanche, il ignore les pièces jointes tel que les images.

Bogofilter est écrit en C, et peut fonctionner sous Linux, FreeBSD, NetBSD, OpenBSD, Solaris, Mac OS X, HP-UX, AIX et d'autres systèmes.

III.15.4. Logiciel anti virus :

Les **antivirus** sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique ne sont qu'une catégorie). Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

III.15.4.1. Fonctionnement :

Un logiciel antivirus vérifie les fichiers et courriers électroniques, les secteur de démarrage (afin de détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont internet), etc.

Différentes méthodes sont possibles :

- Les principaux antivirus du marché se concentrent sur des fichiers et comparent alors la *signature virale* du virus aux codes à vérifier ;
- La *méthode heuristique* est la méthode la plus puissante, tendant à découvrir du code malveillant par son comportement. Elle essaie de le détecter en analysant le code d'un programme inconnu. Parfois de fausses alertes peuvent être provoquées ;
- L'*analyse de forme* repose sur du filtrage basé entre des règles regexp ou autres, mises dans un fichier junk. Cette dernière méthode peut être très efficace pour les serveurs de messagerie électronique supportant les regexp type postfix puisqu'elle ne repose pas sur un fichier de signatures. [7]

Les antivirus peuvent balayer le contenu d'un disque dur, mais également la mémoire vive de l'ordinateur. Pour les antivirus les plus modernes, ils agissent en amont de la machine en scrutant les échanges de fichiers avec l'extérieur, aussi bien en flux descendant (téléchargement) que montant (téléversement ou upload). Ainsi, les courriels sont examinés, mais aussi les fichiers copiés sur ou à partir de supports amovibles tels que cédéroms, disquettes, connexions réseau, clefs USB…

III.15.4.2.Approches :

On distingue plusieurs types de logiciels antivirus selon leur fonctionnement. La première méthode est celle du dictionnaire.

- **Dictionnaire :**

Les créateurs de logiciels antivirus ayant préalablement identifié et enregistré des informations sur des virus, comme le ferait un dictionnaire, le logiciel antivirus peut ainsi détecter et localiser la présence d'un virus. Lorsque cela se produit, l'antivirus dispose de trois options, il peut :

1. effectuer la suppression du fichier contaminé.
2. tenter de réparer le fichier endommagé en éliminant le virus ;
3. déplacer le fichier dans une zone de quarantaine afin qu'il ne puisse être accessible aux autres utilisateurs et logiciels. Ceci permet d'éviter que le virus se répandre (par autoréplication), et permet éventuellement de réparer le fichier ultérieurement ;

Afin de maximiser le rendement de l'antivirus, il est essentiel d'effectuer de fréquentes mises à jour en téléchargeant des versions plus récentes. Des internautes consciencieux et possédant de bonnes connaissances en informatique peuvent identifier eux-mêmes des virus et envoyer leurs informations aux créateurs de logiciels antivirus afin que leur base de données soit mise à jour.

Généralement, les antivirus examinent chaque fichier lorsqu'il est créé, ouvert, fermé ou lu. De cette manière, les virus peuvent être identifiés immédiatement. Il est possible de programmer le système d'administration pour qu'il effectue régulièrement un examen de l'ensemble des fichiers sur l'espace de stockage (disque dur, etc.).

Même si les logiciels antivirus sont très performants et régulièrement mis à jour, les créateurs de virus font tout aussi souvent preuve d'inventivité. En particulier, les virus « oligomorphiques », « polymorphiques » et plus récemment, « métamorphiques », sont plus difficiles à détecter.

- ***Liste blanche* :**

La « liste blanche » est une technique de plus en plus utilisée pour lutter contre les logiciels malveillants. Au lieu de rechercher les logiciels connus comme malveillants, on empêche l'exécution de tout logiciel à l'exception de ceux qui sont considérés comme fiables par l'administrateur système. En adoptant cette méthode de blocage par défaut, on évite les problèmes inhérents à la mise à jour du fichier de signatures virales. De plus, elle permet d'empêcher l'exécution de logiciels indésirables. [7]
Étant donné que les entreprises modernes possèdent de nombreuses applications considérées comme fiables, l'efficacité de cette technique dépend de la capacité de l'administrateur à établir et mettre à jour la liste blanche. Cette tâche peut être facilitée par l'utilisation d'outils d'automatisation des processus d'inventaire et de maintenance.

- **Comportements suspects :**

Une autre approche pour localiser les virus consiste à détecter les comportements suspects des programmes. Par exemple, si un programme tente d'écrire des données sur un programme exécuté, l'antivirus détectera ce comportement suspect et en avisera l'usager qui lui indiquera les mesures à suivre.

Contrairement à l'approche précédente, la méthode du comportement suspect permet d'identifier des virus très récents qui ne seraient pas encore connus dans le dictionnaire de l'antivirus. Toutefois, le fait que les usagers soient constamment avertis de fausses alertes peuvent les rendre insensibles aux véritables menaces. Si les usagers répondent « Accepter » à toutes ces alertes, l'antivirus ne leur procurera aucune protection supplémentaire. Ce problème s'est aggravé depuis 1997, puisque plusieurs programmes inoffensifs ont modifié certains fichiers exécutables sans observer ces fausses alertes. C'est pourquoi, les antivirus les plus modernes utilisent de moins en moins cette méthode.

- **Autres approches :**

L'*analyse heuristique* est utilisée par quelques antivirus. Par exemple, l'antivirus peut analyser le début de chaque code de toutes les nouvelles applications avant de transférer le contrôle à l'usager. Si le programme semble être un virus, alors l'usager en sera averti. Toutefois, cette méthode peut également mener à de fausses alertes. La méthode heuristique permet de détecter des variantes de virus et, en communiquant automatiquement les résultats de l'analyse à l'éditeur, celui-ci peut en vérifier la justesse et mettre à jour sa base de définitions virales.

La *méthode du bac à sable (sandbox en anglais)* consiste à émuler le système d'exploitation et à exécuter le fichier lors de cette simulation. Une fois que le programme prend fin, les logiciels analysent le résultat du bac à sable afin de détecter les changements qui pourraient contenir des virus. En raison des problèmes de performance, ce type de détection a lieu habituellement pendant le balayage sur demande [1]. Cette méthode peut échouer puisque les virus peuvent s'avérer non déterministes et résulter de différentes actions ou même peut-être d'aucune action lorsque exécuté. Il est impossible de le détecter à partir d'une seule exécution.

- **Analyse heuristique**

L'**analyse heuristique** est une méthode utilisée par les logiciels antivirus pour détecter les nouveaux virus, ainsi que les nouvelles variantes d'un virus déjà connu. L'analyse heuristique est une méthode basée sur le comportement supposé d'un programme afin de déterminer si ce dernier est ou non un virus. Cette méthode se différencie de l'analyse statistique qui se base quant à elle sur des comparaisons du programme avec des virus connus référencés dans une bibliothèque du logiciel antivirus.

- ✓ **Fonctionnement :**

Les logiciels antivirus exécutent le code ou le script de fichier à analyser dans un environnement virtuel, tout en analysant les instructions de programme. Cela permet de connaitre le comportement de programme tout en isolant le code du fichier suspect de la machine réelle. Si l'antivirus détecte des instructions suspectes comme la suppression de fichiers, lancement de processus multiple, le fichier sera reconnu comme un virus et l'utilisateur sera alerté. Une autre technique consiste à décompiler le programme en question et analyser son code source. Le code est comparé aux codes d'autres virus connus. Si une grande partie de code est trouvée dans d'autres virus, le programme sera reconnu en tant qu'une menace. L'utilisateur peut lui-même faire une analyse heuristique sans avoir recours à un antivirus en simulant le fonctionnement de celui-ci. Il consiste à lancer le fichier dans une machine virtuelle, et voir le comportement de programme et l'état de la machine. Par exemple, Deep Freeze protège la configuration de l'ordinateur tout en permettant à l'utilisateur de faire tout ce qu'il veut. Les dernières versions de Kaspersky intègrent un bureau virtuel, l'utilisateur peut lancer les applications suspectes en toute sécurité.

Inconvénient :

Bien que l'analyse heuristique permette de détecter de nouveaux virus et les nouvelles variantes de virus préexistants, l'efficacité est vraiment faible au regard du nombre de faux positifs. C'est parce que les virus informatique tout comme les virus biologiques changent

constamment et ils évoluent. Comme l'analyse heuristique se repose sur la comparaison de fichier suspect avec les autres virus déjà connus, il est fréquent qu'elle rate certains virus qui contiennent de nouveaux codes ou de nouvelles méthodes de fonctionnement.

III.16. Logiciel d'analyse du réseau informatique :

- **Analyseur de paquets :**

Un **analyseur de paquets** est un logiciel pouvant lire ou enregistrer des données transitant par le biais d'un réseau local non-commuté. Il permet de capturer chaque paquet du flux de données (en) traversant le réseau, voire, décoder les paquets de données brutes (en), afficher les valeurs des divers champs du paquet, et analyser leur contenu conformément aux spécifications ou RFC appropriées [3]. L'analyseur de paquets permet ainsi la résolution de problèmes réseaux en visualisant ce qui passe à travers l'interface réseau, mais peut également servir à effectuer de la rétro-ingénierie réseau à des buts d'interopérabilité, de sécurité ou de résolution de problème. Il peut aussi être utilisé pour intercepter des mots de passe qui transitent en clair ou toute autre information non-chiffrée pour sa capacité de consultation aisée des données non-chiffrées.

- **Types :**

Les *sniffers* sont des sortes de sondes que l'on place sur un réseau pour l'écouter et en particulier parfois récupérer à la volée des informations sensibles lorsqu'elles ne sont pas chiffrées, comme des mots de passe (parfois sans que les utilisateurs ou les administrateurs du réseau ne s'en rendent compte).

Le renifleur peut être un équipement matériel ou un logiciel : le premier est bien plus puissant et efficace que le second, encore que, la puissance des machines augmentant sans cesse, l'écart se resserre. Mais le premier est surtout beaucoup plus cher que le second.

- **Fonctionnement :**

Lorsqu'une machine veut communiquer avec une autre sur un réseau non-commuté (relié par un hub ou câblé en câble coaxial, qui sont des techniques obsolètes), elle envoie ses messages sur le réseau à l'ensemble des machines et normalement seule la machine destinataire intercepte le message pour le lire, alors que les autres l'ignorent. Ainsi en utilisant la méthode du *sniffing*, il est possible d'écouter le trafic passant par un adaptateur réseau (carte réseau, carte réseau sans fil, etc.).

Pour pouvoir écouter tout le trafic sur une interface réseau, celle-ci doit être configurée dans un mode spécifique, le « mode promiscuous ». Ce mode permet d'écouter tous les paquets passant par l'interface, alors que dans le mode normal, le matériel servant d'interface réseau élimine les paquets n'étant pas à destination de l'hôte. Par exemple, il n'est pas nécessaire de mettre la carte en mode « *promiscuous* » pour avoir accès aux mots de passe transitant sur un serveur FTP, vu que tous les mots de passe sont à destination dudit serveur.

Le *packet sniffer* décompose ces messages et les rassemble, ainsi les informations peuvent être analysées à des fins frauduleuses (détecter des logins, des mots de passe, des emails), analyser un problème réseau, superviser un trafic ou encore faire de la rétro-ingénierie.

- **Sécurité :**

La solution à ce problème d'indiscrétion est d'utiliser des protocoles de communication chiffrés, comme SSH (SFTP, scp), SSL (HTTPS ou FTPS) (et non des protocoles en clair comme HTTP, FTP, Telnet).

La technique du *sniffing* peut être ressentie comme profondément malhonnête et indélicate, mais elle est souvent nécessaire lorsque l'on est à la recherche d'une panne.

III.17. Les logiciels de tests de vulnérabilité et de détection d'erreurs de configuration :

Ils permettent de façon automatique de rechercher les erreurs de configuration ou les vulnérabilités du système (Satan, Colt).

III.18. Sécurité du système d'exploitation :

Système d'exploitation basé sur la sécurité :

Voici la liste alphabétique des systèmes d'exploitation non seulement reconnus pour leur sécurité, mais issus d'un projet axé sur le renforcement de la sécurité. Les critères sont détaillés et peuvent également être répertoriés dans les systèmes d'exploitation évalués.

- **BSD**

BSD (pour Berkeley Software Distribution) est un système d'exploitation sous une licence libre, la licence BSD, duquel sont dérivés NetBSD, FreeBSD et OpenBSD notamment.

- **OpenBSD :** OpenBSD est issu de la séparation avec NetBSD, le plus ancien des trois autres principaux systèmes d'exploitation de la famille des BSD aujourd'hui en activité. C'est un projet open source hautement concerné par la sécurité, il inclut un certain nombre de mesures de sécurité absentes ou optionnelles dans d'autres systèmes d'exploitation, même au détriment de la facilité d'utilisation, de la vitesse ou des fonctionnalités. Des audits de codes considérés comme étant des éléments importants de la sécurité d'un système sont effectués.
- **TrustedBSD :** TrustedBSD est une surcouche de FreeBSD destinée à accentuer la sécurité. Le projet est rendu possible par des subventions venant de différentes organisations; il suit les critères communs pour l'évaluation de sécurité de Trusted Computer System Evaluation Criteria (ensemble de critères énoncés par le Département de la Défense des États-Unis dans le livre orange, ou orange book). Les principaux travaux portent notamment sur le contrôle d'accès discrétionnaire et sur l'implémentation FLASK/TE de la NSA. Beaucoup d'extensions concernant la sécurité ont été intégrées au projet principal, FreeBSD, à partir des versions 5.x. [1]

- **Linux**

Linux est l'appellation courante du système d'exploitation libre, multitâche, multiplate-forme et multi-utilisateur de type Unix basé sur le noyau Linux écrit par Linus Torvalds. Linux n'est pas à proprement parler basé sur la sécurité, mais diverses distributions s'en donnent l'objectif.

- **Adamantix :** Adamantix, aussi connue sous le nom de *Trusted Debian*, est un système d'exploitation GNU/Linux, basé sur Debian, et orienté sécurité avec notamment des protections contre les attaques utilisant des débordements avec PaX et SSP et un contrôle avancé du système à l'aide de RSBAC (Rule Set Based Access Control).
- **Annvix :** Annvix est dérivée de Mandriva pour produire une distribution sécurisée dédiée aux serveurs. Elle emploie la protection Stack-Smashing Protector (SSP) contre des dépassements de tampons mémoire et utilisera prochainement RSBAC (Rule Set Based Access Control).
- **Fedora :** Fedora est un projet basé sur la distribution Red Hat. C'est la seule distribution répandue qui intègre des éléments supplémentaires de sécurité, avec l'intégration du module de sécurité SELinux avec le contrôle d'accès obligatoire (Mandatory access control pour la gestion des droits des utilisateurs, et notamment l'utilisation systématique des préventions de dépassement de tampon.
- **Hardened Gentoo :** Hardened Gentoo est un sous-projet de Gentoo. Sont utilisés le module de sécurité SELinux, le patch PaX contre des dépassements de tampons mémoire, le RSBAC (Rule Set Based Access Control), le patch Grsecurity restreignant les droits d'administrateur et le script Bastille Linux.
- **Immunix :** Immunix est une distribution commerciale utilisant divers systèmes de sécurité lourds. Y figurent StackGuard, la signature et le chiffrement des exécutables.
- **Hardened Linux (Wendzel Linux) :** Wendzel Linux est une petite distribution pour jouer le rôle de pare-feu, de détection d'intrusions et de porte d'accès aux réseaux VPN. La distribution est basée sur la Slackware mais a subi de profondes modifications comme l'utilisation du patch Grsecurity pour le kernel. [1]

- **Solaris**

Solaris est le système d'exploitation Unix propriétaire de Sun Microsystems. Le système en lui-même n'est pas axé sur la sécurité. Des fonctionnalités provenant du projet OpenSolaris comme ZFS sont fusionnés en amont à la version officielle de Solaris après diverses certifications.

- **Trusted Solaris :** Trusted Solaris est principalement utilisée par des instances gouvernementales dans le domaine du calcul. Cette distribution possède des audits détaillés, elle utilise le contrôle d'accès obligatoire (Mandatory access control) avec des méthodes d'authentification physique via des périphériques et le RSBAC (Rule Set Based Access Control). Une partie de ces moyens sécuritaires ont été transférés dans la version Solaris 10. [1]

III.19. Moyens de Lutte anti-spam :

La **lutte antipourriel** (**anti-spam** ou **anti-spamming**, ou **antipollupostage**) est un ensemble de comportements, de systèmes et de moyens techniques et juridiques permettant de combattre le pourriel (ou « spam », courriers électroniques publicitaires non sollicités).

- **L'intérêt de la lutte anti-spam :**

Autour de l'année 2000, le spam pouvait sembler inoffensif. En effet, la plupart des spammeurs utilisaient ce moyen afin de promouvoir des produits en tous genres (produits pharmaceutiques, faux diplômes, logiciels piratés, matériel pornographique, etc.). Or, avec le volume sans cesse croissant de spams transitant dans l'Internet (plus de 90 % des messages),

et avec l'arrivée de types de spams plus pervers, tels l'hameçonnage, où la sécurité financière d'un individu est mise en péril, il est devenu très important de se prémunir contre cette nuisance. [10]

Le spam fait perdre beaucoup d'argent aux entreprises reliés aux problèmes qu'il peut causer aux systèmes informatiques mais aussi au niveau de la perte de temps des employés.

- **Rester anonyme :**

Pour éviter de recevoir du spam, les internautes font souvent figurer leurs adresses email d'une manière masquée lorsqu'elle doit apparaitre dans un site web ou dans Usenet. Par exemple :

- Jean@NOSPAM.exemple.fr pour Jean@exemple.fr.
- Jean chez exemple point fr pour Jean@exemple.fr
- Jean[at]exemple.fr pour Jean@exemple.fr (l'arrobase se prononçant souvent « *at* »).

Mais cette méthode est aussi déconseillée car rien n'interdit au spammeur de faire un traitement d'enlèvement des drapeaux les plus communs (*NOSPAM*, *AT*, *chez* etc.). [16]

Une autre méthode consiste à encoder son adresse avec un algorithme quelconque (par exemple, remplacer chaque lettre par la suivante dans l'alphabet), et d'insérer dans la page une fonction JavaScript qui décode. Ainsi rien ne change pour l'internaute qui peut toujours cliquer sur le lien « envoyer un mail », mais l'adresse n'apparaît pas en clair dans la page. Jusqu'ici, les arroseurs n'exécutent pas le code JavaScript avant de chercher les adresses (trop long, plus complexe, etc.).

Une autre méthode consiste à encoder son adresse en caractères hexadécimaux par exemple : &X02&X36... Cela ne sera pas détectable par les robots qui parcourent les pages web parce qu'ils n'ont pas de moteur de rendu (comme un navigateur web internet explorer, firefox, etc. peut le faire), ils lisent juste des caractères alphanumériques. Il existe de petits logiciels pour faire cela, ou même des codes PHP. L'avantage de cette méthode est que c'est le navigateur qui décode, pas besoin de code javascript.

Enfin, on peut choisir de communiquer son adresse par une image, ainsi on ne pourra pas la récupérer « facilement » par un robot. Pourvu que cette image soit étirée et maquillée afin qu'un logiciel de reconnaissance de caractères (OCR) ne puisse reconstituer votre adresse (sur le même principe qu'un captcha). Cette dernière méthode est considérée comme la plus sûre, bien qu'elle ait pour inconvénient majeur de la rendre très difficile à lire pour des personnes ayant un handicap visuel.

La méthode la plus sûre est sans doute de ne pas divulguer son adresse personnelle sur le Net, lieu public par excellence, mais de la communiquer seulement à vos amis et à vos proches. Et encore, les serveurs de messagerie peuvent parfois être hackés (autre méthode pour les arroseurs pour collecter des adresses).

Plusieurs techniques de lutte contre le spam sont possibles et peuvent être cumulées : filtrage par mots-clés ou par auteur, analyse statistique (méthode bayésienne), listes blanches

(désignation de personnes ou de machines autorisées à publier dans certains lieux), listes noires (désignation de personnes ou de machines auxquelles il est interdit de publier dans certains lieux), interrogation en temps réel de serveurs spécialisés dans la lutte contre le spam.

Ces techniques de lutte, tout comme les logiciels antivirus, doivent s'adapter en permanence car de nouveaux types de spams réussissent à contourner ces défenses.

On distingue généralement deux familles de logiciels antispam :

- Les dispositifs antispam côté client, situé au niveau du client de messagerie. Il s'agit généralement de systèmes possédant des filtres permettant d'identifier, sur la base de règles prédéfinies ou d'un apprentissage (filtres bayésiens). [16]
- Les dispositifs antispam côté serveur, permettant un filtrage du courrier avant remise aux destinataires. Ce type de dispositif est de loin le meilleur car il permet de stopper le courrier non sollicité en amont et éviter l'engorgement des réseaux et des boîtes aux lettres [16]. Une solution intermédiaire consiste à configurer le dispositif antispam du serveur de façon à marquer les messages avec un champ d'en-tête spécifique (par exemple X-Spam-Status: Yes). Grâce à ce marquage, il est aisé de filtrer les messages au niveau du client de messagerie.

En cas d'encombrement ou de saturation totale de la boîte aux lettres, la solution ultime consiste à changer de boîte aux lettres. Il est toutefois conseillé de garder l'ancienne boîte aux lettres pendant un laps de temps suffisant afin de récupérer les adresses de vos contacts et d'être en mesure de communiquer la nouvelle adresse aux seules personnes légitimes.

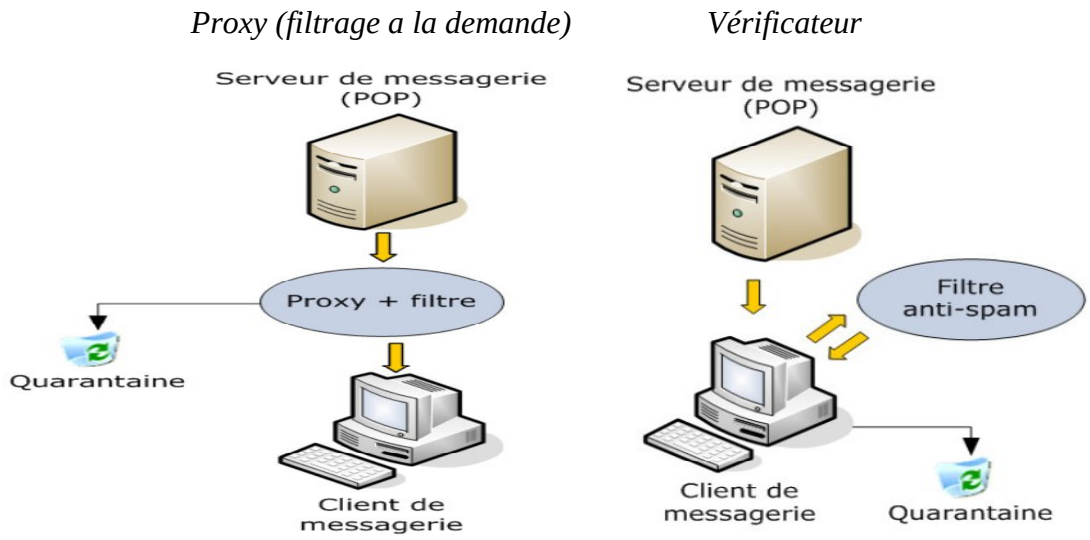


Figure 22 : Les 2 types d'architecture d'integration d'une solution anti spam

III.19.1. Méthodes d'analyse et de filtrage à la réception :

Bien que souvent différentes en matière d'utilisation, d'implantation et de coût, les solutions de lutte anti-spam par filtrage mettent sensiblement les mêmes techniques pour distinguer le spam du courrier légitime. Ces techniques peuvent être mises en œuvre soit au niveau des fournisseurs de service Internet qui protègent leur messagerie, soit au niveau des utilisateurs par des outils appropriés ([filtres anti-spams) [16]. Le filtre est souvent implanté au niveau du MTA (*Mail Transfer Agent*) récepteur du courriel.

Ces techniques peuvent être soit préventives (marquage du courrier pour indiquer qu'il s'agit de courriers indésirables) soit curatives (blocage, voire renvoi des messages incriminés vers l'expéditeur). Cette dernière comporte des inconvénients puisque le destinataire doit pouvoir être maître des courriers qu'il souhaite recevoir. De plus renvoyer un message peut empirer la situation en occupant un peu plus le réseau, avec de fortes probabilités que l'auteur du spam ait maquillé sa véritable adresse ou utilisé l'adresse d'un tiers (tout à fait innocent) comme adresse de retour. De plus, cette façon de faire indique au spammeur que l'adresse visée est bien active, ce qui augmente bien souvent les envois.

Ces outils peuvent être divisés en deux groupes : le filtrage d'enveloppe, et le filtrage de contenu. L'en-tête du courriel constitue les informations de base de ce dernier : expéditeur, destinataire, copie conforme, copie conforme invisible, date d'envoi, serveur source, sujet. Le contenu du message est le message en tant que tel : texte, images, code HTML, etc.

III.19.1.1. Filtrage d'enveloppe :

Le taux d'efficacité du filtrage d'enveloppe est d'environ 50 %. Ce type de filtrage s'applique uniquement à l'en-tête du message, qui contient souvent assez d'informations pour pouvoir distinguer un spam. Il ne s'attache pas au contenu du courriel.

Cette technique présente l'avantage de pouvoir bloquer les courriels avant même que leur corps ne soit envoyé, ce qui diminue grandement le trafic sur la passerelle SMTP (puisque le corps du message est envoyé après que l'en-tête a été reçu et accepté). De plus, le taux de faux positifs dans ce type de filtrage est quasiment nul : lorsqu'un filtre d'enveloppe a identifié un courriel comme du spam, il se trompe rarement.

III.19.1.2.Filtrage de contenu :

Les filtres de contenu analysent le contenu des messages et détectent les spams qui ont réussi à passer à travers le filtre d'enveloppe. Le filtrage de contenu est un peu plus sensible que le filtre d'enveloppe : après tout, les informations véhiculées à travers le message sont subjectives, et ce qui peut paraître un spam selon le filtre de contenu peut être un courriel tout à fait légitime (c'est ce que l'on appelle un faux positif), et l'inverse est aussi vrai (faux-négatif). Le filtrage de contenu peut se développer en plusieurs couches. Par exemple, le filtre peut faire appel à un logiciel antivirus, à un désarchiveur pour analyser les fichiers archivés s'il y a lieu, à un analyseur bayésien, et ainsi de suite.

Exemples de filtre de contenu : SpamAssassin, j-chkmail.

III.19.1.3. Filtrage bayesien :

Le **filtrage bayésien du spam** (en référence au théorème de Bayes) est une technique statistique de détection de pourriels s'appuyant sur la classification naïve bayésienne.

Les filtres bayésiens fonctionnent en établissant une corrélation entre la présence de certains éléments (en général des mots, parfois d'autres choses) dans un message et le fait qu'ils apparaissent en général dans des messages indésirables (*spam*) ou dans des messages légitimes (*ham*) pour calculer la probabilité que ce message soit un spam. [16]

Le filtrage bayésien du spam est une technique puissante pour traiter le courrier électronique indésirable. Elle s'adapte aux habitudes de courrier des uns et des autres et produit un taux de faux positifs suffisamment bas pour être acceptable.

De nombreux agents de courriers électronique modernes mettent en œuvre des filtres bayésiens antispam. Les utilisateurs peuvent également installer des logiciels tiers spécialisé dans ce travail. Il est également possible de déployer ce type de filtres sur les serveurs à l'aide de logiciels spécialisés comme DSpam, SpamAssassin, SpamBayes, Bogofilter ou encore ASSP, et cette fonctionnalité est parfois intégrée au serveur de courrier lui-même.

- **Inconvénients :**

L'empoisonnement bayésien (*bayesian poisoning*) est une technique utilisée par les spameurs pour tenter de dégrader l'efficacité des filtres antispams bayésiens. Elle consiste à placer dans le courrier une grande quantité de texte anodin (provenant de site d'actualités ou de la littérature par exemple), ou bien de salade textuelle (des séquences aléatoires de mots qui semblent cohérentes mais qui ne veulent rien dire), pour noyer le texte indésirable et tromper le filtre. [16]

Les spammeurs peuvent également transformer les mots qui n'apparaissent d'habitude en grande majorité que dans le spam. Ainsi, « Viagra » sera transformé par exemple en « Viaagra » ou en « V!agra ». La lecture reste toujours possible par le destinataire mais chacun de ces mots transformés ne se rencontrera que plus rarement, ce qui pénalise l'apprentissage par le filtre bayésien. En pratique, cette technique marche assez mal, car les mots dérivés finissent eux-mêmes par être reconnus par le filtre.

Une autre technique utilisée par les spammeurs pour essayer de tromper le filtre bayésien est de remplacer le texte par des images. L'ensemble du texte, ou une partie de celui-ci, est remplacé par une image où ce même texte est « dessiné ». Le filtre de spam est d'ordinaire incapable d'analyser cette image qui contient les mots sensibles comme « Viagra ». Néanmoins, bon nombre d'utilisateurs désactivent l'affichage des images pour des raisons de sécurité, ce qui fait que les polluposteurs atteignent moins leurs cibles. De plus, la taille d'une image est supérieure à celle du texte équivalent, et les polluposteurs ont besoin de plus de bande passante pour envoyer des messages contenant des images. Certains filtres tendent à décider qu'un message est du spam quand il a trop de contenu graphique. Enfin, une solution qui est probablement plus efficace a été proposée par Google et est utilisée par le système de courrier électronique Gmail : traiter toute image de taille moyenne ou grande par reconnaissance optique de caractères pour analyser le texte qu'elle contient[11].

III.19.1.4. Filtrage par mots-clés ou adresses :

Cette méthode est très limitée car elle se base sur le rejet ou le tri du courrier en fonction de règles de vocabulaire préalablement établies, définissant des mots comme interdits. Certains mots-clés revenant souvent dans les spams, tels que « sexe », « viagra » ou « money » pourront servir de base pour la constitution de ces règles. De même on pourra décider de bloquer tous les messages en provenance d'un expéditeur précis, d'un domaine spécifique, voire d'un pays entier.

Cette méthode engendre de fortes probabilités d'erreur et s'avère peu efficace lorsque les spammeurs maquillent les mots utilisés (« vi@gr@ », « s3x », etc.). Il convient alors d'utiliser les expressions rationnelles.

III.19.1.5. Filtrage par expressions rationnelles :

Une expression rationnelle (appelée souvent « expression régulière » en informatique) est un motif que l'on peut appliquer à une chaîne afin de voir si ladite chaîne correspond au motif (par exemple : un chiffre suivi de trois lettres suivi d'un d'espace, puis d'un chiffre pourrait s'écrire de cette manière : /^[0-9]{1}[A-Za-z]{3} [0-9]{1}$/). En utilisant des expressions rationnelles afin de trouver des variations de mots « sensibles », on augmente les chances de découvrir des spams. Par exemple, si un spammeur tente de déjouer un filtre de mots-clés en utilisant le mot « viiaaagraa », l'expression rationnelle /^vi+a+gra+$/i (un « v » suivi d'un ou plusieurs « i » suivi d'un ou plusieurs « a », suivi d'un « g », d'un « r », et de un ou plusieurs « a », sans se soucier de la casse) permet de retrouver le mot [16]. Évidemment, cet exemple est très simple, mais les expressions rationnelles complexes permettent de détecter des expressions et des déclinaisons beaucoup plus subtiles et sophistiquées.

Une limite de l'utilisation d'expressions rationnelles est illustrée dans le problème de Scunthorpe, qui produit des faux positifs.

III.19.1.6. Filtrage heuristique :

Le filtrage heuristique teste le contenu du message (par exemple, quelle proportion de code HTML, d'images, de références à la pornographie, à l'acquisition facile d'argent contient-il par rapport au reste du message ? le sujet est-il vide ? L'identificateur du message (*Message-ID*) contient-il des signes *« dollar »* (souvent utilisé par les logiciels d'envoi de spams)). Chaque test donne un nombre de points (plus le total est bas, mieux c'est ; moins le message est considéré comme du spam) [10]. Le seuil de points reste arbitraire et défini par l'*administrateur système* qui doit trouver le score donnant le meilleur équilibre entre le nombre de faux positifs et de faux-négatifs.

III.19.1.7. Analyse de virus et de pièces jointes :

Les courriels possèdent souvent des pièces jointes, et celles-ci peuvent contenir des virus. Il est donc important d'avoir, dans le processus de tri des messages, un antivirus. Souvent, les filtres de contenu en ont un intégré. Par exemple, il n'est pas rare de voir SpamAssassin et ClamAV ensemble.

III.19.1.8. Les images :

Les images sont une des difficultés majeures qu'ont à affronter les filtres de contenu. En effet, il est pratiquement impossible de déterminer si l'image est légitime ou non (souvent, les spammeurs utiliseront des images afin de camoufler du texte). Une des techniques pour déterminer, à partir d'une image, si le courriel est légitime ou non, est de regarder le nombre d'images dans le courriel et de voir comment elles sont placées dans le message. Cela peut être un bon indice de la nature du message. Par ailleurs, il est possible de générer une somme de contrôle sur l'image et de la comparer avec d'autres sommes de contrôle disponibles sur Internet (un peu à la manière des RBL). Cela permettra au système de vérifier si l'image a déjà été utilisée dans un spam et de classer le courriel en conséquence. (voir aussi Spam image)

III.19.1.9.Intégrité SMTP :

Les courriels transitant grâce au protocole SMTP, une grande quantité de normes ont été définies pour ce protocole (RFC2821), que les spammeurs omettent souvent de respecter. Par exemple, le nom serveur qui envoie le courriel doit être, préférablement, pleinement qualifié (FQDN) (exemple : mail.domaine.com), règle que les spammeurs ne suivent pas toujours. De même, certains spammeurs usurpent le serveur d'envoi en faisant croire au filtre que le message vient d'un serveur connu (127.0.0.1, par exemple) [16]. Un bon filtre est capable de détecter ces usurpations. Autre exemple : certains spams n'émettent pas de bannière de présentation (HELO), ce qui est pourtant exigé dans les normes SMTP [10]. Ces tests sont laissés à la discrétion du filtre et de l'administrateur système, qui décide quelles sont les règles pertinentes pour son serveur de messagerie. Les règles d'intégrité SMTP sont souvent très efficaces, car, pour les spammeurs, elles agissent comme inhibiteurs de performance (elles ralentissent les envois). Or, un spammeur a intérêt à être le plus performant possible et il peut être très payant pour lui de passer outre ces règles.

III.19.1.10.RPD (« Recurrent Pattern Detection »):

La technologie RPD, *Recurrent Pattern Detection* ou « Détection des signatures récurrentes » en français, est une technologie qui se base non pas sur le contenu des courriels, mais sur leur taux de propagation sur l'ensemble du réseau Internet. Grâce à des serveurs basés un peu partout dans le monde, il est en effet possible de déterminer très rapidement si un courriel est un spam en vérifiant de manière centralisée le nombre de fois où ce même courriel aura été envoyé sur la toile [16]. Si par exemple le même courriel a été envoyé en 100 000 exemplaires en même temps, il s'agira forcément d'un spam.

Cette technologie offre un taux de capture de plus de 98 % des spams pour 1 faux positif sur 1 million).

III.19.2. Méthodes consistant à rendre l'envoi du spam difficile :

- **Filtrage de serveur expéditeur**

Ce type de filtrage permet de bannir des adresses courriel, des domaines, ou des serveurs. Ainsi, tout message provenant d'éléments de la liste noire sera bloqué par le système anti-spam. Ces éléments de liste sont très souvent définis par un administrateur système qui, par expérience, est en mesure de déterminer les sources les plus communes de spam. Cette technique a pour caractéristique de n'être pas limitée qu'au spam dans le sens pur et dur du terme : elle peut également bloquer des sources de courriel légitime, si l'administrateur système les considère comme nuisible [10]. Évidemment, ce type de filtrage est hautement subjectif et dépend du bon vouloir et de l'assiduité de la personne créant la liste.

- **RBL**

Les *Realtime Blackhole List* (RBL) ont comme mandat de fournir une liste de serveurs réputés comme grands envoyeurs de spams, et de lister les grands spammeurs. Il s'agit en fait d'une grande liste noire généralisée [1]. Le principe d'utilisation est simple : lorsqu'un filtre reçoit un courriel, il vérifie si le serveur d'envoi est contenu dans un RBL. Si oui, le courriel est catégorisé comme spam.

- **SPF (« Sender Policy Framework »)**

SPF (*Sender Policy Framework*) se base sur la zone DNS d'un domaine pour fonctionner. Le détenteur d'un domaine ajoute, dans la zone DNS de ce domaine, un enregistrement de type TXT qui indique quelles sont les machines autorisées ou non à envoyer du courriel pour le domaine. Ainsi, si mail.domainea.com est le seul serveur autorisé à envoyer du courriel pour domainea.com, ce sera spécifié dans l'enregistrement TXT. Pour fonctionner correctement, le support SPF doit être activé sur le filtre antispam [10]. Le système vérifie que le serveur envoyant le courriel est bien dans la liste des serveurs autorisés. Sinon, il s'agit d'un spam.

- **Liste grise (*Greylisting*)**

La liste grise est un terme utilisé pour décrire une technologie antispam particulièrement efficace, qui fonctionne selon ce principe : selon les normes définies dans le RFC 2821, lorsqu'un serveur de réception de courriel (dans ce cas-ci, le serveur qui reçoit le courriel, sur lequel le filtre de courriel est activé) ne peut traiter la réception d'un message (par exemple, s'il est indisponible), il doit retourner un code d'erreur 421. Ce code d'erreur indique au serveur qui envoie le message d'attendre et de réessayer l'envoi un peu plus tard. Ce délai est défini dans la configuration du serveur expéditeur du message (ou *Mail Transfert Agent*). Tout MTA légitime respecte cette règle. Les MTA non légitimes (utilisés par les spammeurs) ne le font pas car cela leur fait perdre de l'efficacité : le MTA continue donc son envoi de courriels (il passe au prochain destinataire) sans attendre pour ré-envoyer le courriel actuel. [16]

Les experts de la sécurité du courriel ont donc envisagé une méthode exploitant cette particularité : la liste grise. Celle-ci fonctionne avec une base de données. Chaque enregistrement de la base de données constitue un triplet composé de l'adresse IP du serveur qui envoie le courriel, de l'adresse courriel de l'expéditeur, et de l'adresse courriel du destinataire, formant ainsi une clé unique. Est aussi stockée dans la base la date de la première connexion du triplet au serveur. Lorsqu'un message est reçu par le serveur de courriel du destinataire, ce dernier vérifie dans sa base l'existence du triplet.

- Si le triplet n'est pas dans sa base de données, il l'ajoute avec la date actuelle. Il renvoie ensuite le code d'erreur 421, indiquant au serveur qu'il devra ré-envoyer le message.
- Si le triplet est déjà dans la base de données, le serveur vérifie le délai entre la date courante et celle stockée dans la base (la date de la première connexion). Si le délai est supérieur ou égal à un délai prédéfini (par exemple, 5 minutes), le message est accepté. Sinon, le serveur retourne un numéro d'erreur 421.

Après un certain temps (défini également dans l'enregistrement), l'enregistrement devient inactif et le serveur doit ré-envoyer un 421 (on peut supposer que l'enregistrement est détruit). Ainsi, lorsque le MTA envoyeur reçoit le 421, s'il est légitime, il attendra avant de ré-envoyer le message. Sinon, il n'attendra pas et ne le ré-enverra pas.

Cette technique permettait d'atteindre des taux d'efficacité très élevés, de l'ordre de 99 % quand elle a été proposée en 2003, puisque la très grande majorité des spammeurs préfère sacrifier un courriel plutôt que d'attendre et ainsi, diminuer leur performance. Actuellement l'efficacité est moins importante (~80-90 %) à cause de l'augmentation de l'utilisation des webmails (des vrais serveurs de messagerie), par les spammeurs, pour distribuer les spams.

Cette méthode a également un effet secondaire inattendu : elle est relativement efficace pour supprimer les vers utilisant la messagerie pour se propager. C'est une qualité partagée par les méthodes de filtrage dite « protocolaires », telles la limitation de cadences, les RBL et les listes de réputation.

- **Captcha**

Dans les méthodes à base de Captcha, l'expéditeur d'un courriel doit prouver son « humanité » en recopiant un mot affiché sous forme d'une image, un captcha. Un robot spammeur ne saura pas recopier ce mot alors qu'un humain pourra le faire très facilement et sera alors autorisé une fois pour toutes à écrire à son correspondant.

- **Priorité des enregistrements MX**

Lors de la définition de la zone DNS pour un domaine, il est possible de définir un enregistrement MX (*Mail EXchanger*), qui spécifie quel est le serveur responsable de la gestion du courriel pour le dit domaine. Il est possible de définir plusieurs enregistrements MX, de sorte que si l'un tombe, un autre pourra prendre le relais. À chaque enregistrement est associé un nombre indiquant une priorité (exemple, 10, 20, 30, 100, 200, etc.). Les MTA sont tenus d'envoyer leur courrier au serveur le plus prioritaire (celui qui a le nombre le plus bas). De fait, il est tout à fait normal que le serveur ayant la plus haute priorité soit le plus sollicité. Ainsi, c'est souvent lui qui sera le plus sécurisé (les autres le seront souvent moins). Les spammeurs ont vite fait de découvrir cette situation et il n'est pas rare que les spams soient envoyés au serveur ayant la plus faible priorité (le nombre le plus élevé). Ces serveurs étant souvent moins protégés, la probabilité qu'un spam passe est donc plus élevée. Pour contrer ce problème, il est fortement conseillé de protéger tous ses MX de la même manière. De plus, il est possible de déjouer les spammeurs en spécifiant dans le MX le plus élevé un serveur factice. Plus spécifiquement, ce serveur pourrait rejeter toutes les connexions, et donc, toutes les tentatives de spams se rendant au serveur seraient déjouées.

- **Rendre les courriels payants**

Mettre un prix sur l'envoi de courriels, symbolique pour les envois légitimes mais dissuasif pour les envois massifs (à 2 centimes d'euros par courrier, celui-ci reste toutefois du même ordre de coût pour l'expéditeur qu'une publicité radio ; or elle peut être « bien mieux ciblée » selon l'endroit où a été récoltée l'adresse). Et à 20 centimes d'euros il sera nécessaire de mettre une franchise sinon c'est l'accès à l'envoi de courrier pour le particulier au budget le plus serré qui commence à s'estomper.

En 2005, l'homme politique Alain Lamassoure (UMP), alors député européen, avait proposé de taxer les courriels (0,00001 centime) pour financer l'Union européenne[7]. Il s'agissait d'un malentendu, qui a donné lieu en 2011 à un canular informatique sur le même thème. [1]

- **Modération**

Dans les forums Internet et Usenet, ainsi que sur les listes de diffusion, on a souvent recours à la modération : une personne de confiance (« modérateur ») lit les messages dont la publication est proposée, et refuse éventuellement de les diffuser (modération *a priori*) ; ou bien cette personne lit les messages qui ont déjà été diffusés, et efface ceux qui lui semblent hors de propos (modération *a posteriori*) [16]. Comme cette méthode nécessite des moyens

humains importants, et que de plus les modérateurs sont souvent accusés (de censure) à outrance, il existe aussi une modération par robot (généralement appelée « robot-modération ») : n'importe qui peut publier un message par l'intermédiaire du robot, même si cet article est dépourvu d'intérêt (et même s'il constitue effectivement un pollupostage), mais le robot ne laisse passer le message que s'il répond à un critère simple et connu de tous, comme la présence d'un certain mot dans son titre. Cette protection est surtout efficace contre les robots qui émettent automatiquement des messages identiques dans des dizaines de forums, et qui n'ont pas été programmés pour produire des messages conformes aux exigences spécifiques de tel ou tel forum.

III.20. Conclusion :

Obtenir un niveau de sécurité informatique suffisant pour prévenir les risques technologique et informationnel est primordial pour le bon fonctionnement des entreprises.

Il est important de pouvoir les identifiés correctement pour circonscrire le périmètre de sécurité à mettre en place et protéger efficacement les valeurs qui doivent l'être.
Dans ce chapitre, nous avons présenté les différentes techniques et mécanismes de défense (*qui vont de la protection des machines des utilisateurs à la protection de tout le réseau, en passant par des mécanismes dédiés exclusivement à la protection des serveurs*) pour parer bien sûr aux attaques des pirates.

La sécurisation des systèmes informatiques d'une entreprise est devenue une nécessité pour son épanouissement et développement qu'il faut prendre en considération en lui réservant une partie de son budget de l'entreprise afin de l'améliorer.

Dans ce chapitre nous avons étudié la SSI sous l'angle technique, dans le chapitre suivant nous l'étudierons sous l'angle organisationnel pour pouvoir mettre en place une politique de sécurité basée sur la technique, l'organisation et la sensibilisation.

Chapitre IV : Mise en place d'une politique de sécurité informatique (PSSI)

VI.1. Introduction :

La sécurité des systèmes d'information se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système, en mettant en place des mécanismes d'authentification et de contrôle. Ces mécanismes permettent d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.

La sécurité informatique doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, c'est-à-dire :

- ✓ élaborer des règles et des procédures, installer des outils techniques dans les différents services de l'organisation (autour de l'informatique) ;
- ✓ définir les actions à entreprendre et les personnes à contacter en cas de détection d'une intrusion ;
- ✓ sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'informations ;
- ✓ préciser les rôles et responsabilités.

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

IV.2. Dé inition:

La **politique de sécurité des systèmes d'information** (PSSI) est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration, État, unions d'États …) en matière de sécurité des systèmes d'information (SSI). [1]

IV.3. Schéma directeur :

Il est important de connaître la criticité des informations transitant dans le système d'information. Il est donc nécessaire d'avoir une approche et connaissance technique des systèmes déployés, mais également une mise en place de processus décrivant les enjeux de la sécurité des systèmes d'information au niveau organisationnel et juridique. La liste des différents processus nécessaires peuvent être déployés en fonction de normes ISO et méthodes ou bonnes pratiques. Afin de décrire et vulgariser au mieux l'ensemble de ces procédures, il est possible de les centraliser dans un document appelé *schéma directeur de la sécurité des*

systèmes d'information (SDSSI). Ce document permet de décrire la sécurité des systèmes d'information liée à la stratégie de l'entreprise. [17]

Avant tout déploiement de solutions technique, il est préférable de se référer à ce type de document régissant la politique de sécurité générale de l'entité.

Nous pouvons prendre en compte trois éléments incontournables dans la mise en place d'un SDSSI:

- **L'implication de la direction :**

  Il est nécessaire que les dirigeants et responsables de départements soient les premiers à être impliqués dans la mise en place du SDSSI, cela pour trois raisons. La première concerne la criticité des informations contenues dans les systèmes d'information. En effet, seule la direction est en mesure de graduer la priorité et criticité des informations contenues dans les système d'information. La seconde concerne la mise à disposition de ressources (financières / humaines) pour la mise en place de cette politique. La troisième et dernière raison permet *"d'imposer"* à l'ensemble des salariés ce nouveau fonctionnement. [A7]

- **L'implication des utilisateurs :**

  Même si la direction appuie la mise en place d'une politique efficace en terme de sécurité des systèmes d'information, il est souvent nécessaire d'insister plus lourdement envers les salariés. Cependant, l'approche n'est pas la même que pour la direction. Les salariés on souvent plus de mal à changer leurs habitudes (cas vécu) et ne comprennent pas l'importance de la mise en place d'une sécurité, même infime. L'approche ici doit être vulgarisée au maximum et prend souvent beaucoup de temps.

- **La criticité des informations et des services :**

  Il est indispensable pour chaque information et service du système d'information, d'évaluer sa sensibilité, les menaces pesant sur cette ressource et la gravité de ces menaces.

  Pour chaque ressource il est important de déterminer l'importance de sa disponibilité, de son intégrité et de sa confidentialité.

Ce document est le moins technique possible afin d'être compris par l'ensemble de l'entreprise, et des prestataires par exemple. Cependant, il est intéressant de spécifier des éléments comme la politique liées au mot de passe (juste pour éviter les *pourquoi je ne peux pas mettre ma date de naissance, ou pourquoi c'est un problème de l'indiquer sur post-it sous le clavier alors qu'il n'y a que moi qui sais ...*). On pourrait donc intégrer la nécessité de posséder un mot de passe de plus de 7 caractères composé alpha-numériquement avec des caractères spéciaux (en expliquant pourquoi), que chaque mot de passe est conservé par une seule et même personne dans un espace chiffré, et que cette donnée sera renouvelée tous les ans.

IV.4. Elaboration d'un tableau de bord :

Un tableau de bord parfaitement adapté à chaque type de fonction de la "voie fonctionnelle SSI" est un atout pour améliorer la qualité des services de sécurité et maîtriser le niveau de sécurité global de sécurité des systèmes d'information.

Il constitue en effet un outil de synthèse et de visualisation indispensable pour suivre toutes les actions liées à la SSI. Il contribue à contrôler que la stratégie définie dans la politique de sécurité est mise en œuvre par les niveaux de pilotage et opérationnel, et à la remontée d'informations pertinentes jusqu'aux décideurs. [17]

Pour le niveau stratégique, la mise en place d'un tableau de bord SSI permet de:

- suivre l'application de la politique de sécurité,
- établir des comparaisons avec d'autres organismes,
- préparer les choix de mise en place des ressources (définition de priorités, réévaluation de la menace et du risque).

Pour le niveau de pilotage, la mise en place d'un tableau de bord SSI permet de :

- contrôler la réalisation des objectifs par le niveau opérationnel,
- améliorer la qualité de service.

Pour le niveau opérationnel, la mise en place d'un tableau de bord SSI permet de :

- préciser les besoins opérationnels à mettre en œuvre,
- mesurer la production et les efforts entrepris pour atteindre les objectifs visés en matière de production,
- motiver et dynamiser les équipes.

IV.5. Organisation dans l'entreprise :

Pour une bonne mise en œuvre de la SSI dans une entreprise, il est nécessaire de s'adosser à des technologies SSI existantes, et surtout, d'associer l'ensemble du personnel dans cette démarche de sécurisation SSI et de définir des méthodes de travail conformes à la politique de l'entreprise.

En effet, pourquoi sécuriser un SI, à l'aide de solutions sophistiquées si les employés ont la possibilité de désactiver des options de sécurité qui leur paraissent gênantes dans la réalisation de leurs tâches ?

Pourquoi sécuriser une base LDAP de mots de passe, si les employés divulguent leur login/mot de passe à toute personne se faisant passer au téléphone pour l'administrateur du réseau de l'entreprise ? [18]

Les exemples d'ingénierie sociale sont nombreux .pour se prémunir de telles vulnérabilité qui, notons le, ne mettent pas en défaut le système SSI lui-même, mais le comportement du personnel, une entreprise n'a pas d'autres chois que de sensibiliser, et former, l'ensemble de son personnel à la problématique de SSI.

Pour assurer un bon suivi de son SSI, une entreprise se doit de nommer un, ou plusieurs responsable(s) SSI (RSSI). Le RSSI a pour fonction de :

- Maintenir ou renforcer la SSI en fonction des risques encourus et des potentielles pertes occasionnés.
- Participer au processus d'arbitrage du budget alloué à la SSI
- Définir une politique SSI et une charte SSI [A6]

Il a donc une double casquette :

- Associer le personnel à la démarche SSI
- Mettre en œuvre les moyennes techniques SSI dans le système informatique de l'entreprise en adéquation avec le budget alloué et les exigences de sécurité [A6]

Etant donné son rôle central dans le SI, il est fortement conseillé qu'il soit directement rattaché a la direction générale et ce pour lui permettre d'en référer directement a la DG, en particulier quand un incident grave de sécurité peut aller jusqu'à remettre en cause l'action de l'entreprise.

IV.6. Politique de sécurité :

La structure générale d'une politique de sécurité peut aborder les points suivants :

- **Organisation et responsabilités :** La PSSI précise l'organisation des fonctions chargées de la sécurité au sein de l'entreprise (postes, rattachements, répartition géographique, cumul, etc.) ainsi que les prérogatives associées à ces fonctions (conduite d'audit, ouverture des services, attribution des droits, gestion des habilitations, etc.).
- **Intégration et interactions de la SSI :** La PSSI doit également prévoir les modalités d'intégration des fonctions SSI dans l'entreprise et notamment :
  - la manière dont la SSI est prise en compte dans les projets menés par l'entreprise (notamment les projets de développement de logiciels s'il y en a) ainsi que dans les choix techniques effectués (sélection de logiciels, etc.) ;
  - et la manière dont la SSI interagit avec les services chargés de l'exploitation des systèmes informatiques (priorités, indépendance ou non, acquisition des matériels, budget, etc.).
- **Objectifs de sécurité :** La PSSI doit définir les objectifs de sécurité de haut niveau de l'entreprise. Par exemple, c'est à ce niveau que peut être imposé l'utilisation de systèmes d'authentification à deux facteurs, la nécessité de l'agrément sécurité des serveurs pour certains domaines d'activité, la prédominance de la disponibilité sur les autres aspects de la sécurité (ou l'inverse - ce qui est quand même plus rare), etc. Les objectifs de sécurité, validés par la direction générale, révèlent les intentions de l'ensemble de l'entreprise en terme de sécurité informatique et légitiment les efforts concrets de mise en place. (C'est notamment en ce sens que la PSSI est un document « politique ».)
- **Règles générales de sécurité** : La PSSI doit non seulement identifier les objectifs assignés, mais également les règles de sécurité générales qu'elles imposent, parmi lesquelles on retrouve certains points récurrents : l'attribution d'un identifiant aux employés, la gestion de leurs habilitations, les règles de rattachement au réseau, la contractualisation des règles avec des partenaires extérieurs. Mais on peut également définir à ce niveau des règles spécifiques : la délégation de certains droits, les autorisations d'ouverture de services réseau, le type des systèmes d'authentification autorisés, la nationalité des fournisseurs, la gestion des obligations légales (traitement de données personnelles notamment), etc.

- **Gestion des risques :** Les objectifs de sécurité correspondent à des décisions volontaires, mais celles-ci sont bien entendu motivées par les risques encourus par l'entreprise. Idéalement, les objectifs de sécurité doivent correspondre aux mesures permettant de limiter tous les risques majeurs associés à des défaillances de sécurité du système d'information. Mais des risques résiduels existent généralement et la PSSI peut aborder le sujet de la gestion des risques notamment si des efforts d'analyse des risques ou d'audit interne sont menés dans l'entreprise (c'est peut-être déjà le cas, notamment vis à vis du risque financier).

Par rapport à cette structure, la PSSI peut aborder un certain nombre de thèmes correspondant aux principaux domaines techniques du système informatique et du système d'information qu'il me en œuvre. On y recense notamment les thèmes suivants :

- la protection des communications (informatiques mais aussi téléphoniques) ;
- la gestion des violations (blocage, arrêt, correction, suivi, voire sanction) ;
- les interactions avec le domaine de la vie privée - régi en France par la loi de protection des traitements de données à caractère personnel ;
- les procédures de choix et d'achats de matériels ;
- la gestion de la messagerie, notamment si celle-ci est utilisée dans des cas où l'entreprise peut se trouver engagée (par exemple vis à vis d'un sous-traitant) ;
- les procédures de maintenance et d'intervention sur les systèmes en exploitation ;
- les modalités d'enquête et de contrôle de la sécurité ;
- les règles d'identification employées dans le système d'information (les employés permanents constituent le cas le plus simple ; il est loin d'être le seul : intermittents, délégataires, machines, sous-traitants, partenaires, etc.) ;
- les systèmes d'authentification associés à la SSI ;
- les moyens de surveillance mise en place ;
- les systèmes de contrôle d'accès utilisables ;
- la manière dont les contraintes de disponibilité doivent être prises en compte ;
- les règles de gestion du réseau du point de vue de la sécurité (par exemple, point d'accès unique, etc.) ;
- etc.

Les caractéristiques d'une PSSI de bonne qualité sont les suivantes :

- Les objectifs et les règles énoncées doivent être réalistes. Il est inutile de prescrire des obligations ou des interdictions qui gênent tellement le fonctionnement des systèmes que les utilisateurs seront obligées de les contourner pour mener à bien leur mission.
- La PSSI doit être applicable, avec des moyens nécessairement limités (notamment du point de vue humain). En général, ceci impose d'accepter certains compromis de réalisation, et même certaines vulnérabilités.
- La politique doit correspondre à une vision à long terme. Ce type de document ne peut pas être révisé tous les ans. Il doit donc être suffisamment générique pour rester en application quelques années. Les détails sont à préciser dans des documents dérivés.
- La clarté et la concision sont nécessaires à certains moments pour énoncer des règles claires. (En général, celles-ci nécessitent toutefois plusieurs paragraphes d'explication pour être bien comprises, notamment dans différents contextes.)
- La PSSI (et notamment ses règles) doit être basée sur des rôles ou des profils d'utilisateurs : les systèmes changent, la notion même d'utilisateur (au sens informatique)

peut changer pour des raisons techniques, il faut s'appuyer des notions un peu plus abstraites pour définir les règles de sécurité impliquant les droits1 des utilisateurs.

- La PSSI doit permettre une définition claire des domaines de responsabilité et d'autorité, notamment sur les systèmes techniques. L'objectif est alors de pouvoir trancher efficacement entre des points de vue contradictoires (ce qui, dans ce domaine technique, est très fréquent).
- La PSSI doit être à jour (elle doit être revue périodiquement ou quand les évolutions de l'entreprise le nécessitent). C'est probablement assez difficile à assurer.

La PSSI doit être communiquée à tout le personnel pour lui permettre de comprendre dans le détail l'impact de la SSI dans son entreprise et la manière dont il a été décidé de la gérer [A7]. Cette diffusion de la PSSI peut parfois être plus difficile à réaliser, notamment si les objectifs adoptés négligent explicitement certains risques.

IV.7. Audit de sécurité :

L'**audit de sécurité** d'un système d'information (SI) est une vue à un instant *T* de tout ou partie du SI, permettant de comparer l'état du SI à un référentiel.

L'audit répertorie les points forts, et surtout les points faibles (vulnérabilités) de tout ou partie du système. L'auditeur dresse également une série de recommandations pour supprimer les vulnérabilités découvertes. L'audit est généralement réalisé conjointement à une analyse de risques, et par rapport au référentiel. Le référentiel est généralement constitué de :

- la politique de sécurité du système d'information (PSSI)
- la base documentaire du SI
- réglementations propre à l'entreprise
- textes de loi
- documents de référence dans le domaine de la sécurité informatique

IV.7.1. Pourquoi un audit de sécurité ?

L'audit peut être effectué dans différents buts :

- réagir à une attaque
- se faire une bonne idée du niveau de sécurité du SI
- tester la mise en place effective de la PSSI
- tester un nouvel équipement
- évaluer l'évolution de la sécurité (implique un audit périodique)

Dans tous les cas, il a pour but de *vérifier* la sécurité. Dans le cycle de sécurisation, la vérification intervient après la réalisation d'une action. Par exemple, lors de la mise en place d'un nouveau composant dans le SI, il est bon de tester sa sécurité après avoir intégré le composant dans un environnement de test, et avant sa mise en œuvre effective. La roue de Deming illustre ce principe.

Le résultat est le rapport d'audit. Celui-ci contient la liste exhaustive des vulnérabilités recensées par l'auditeur sur le système analysé. Il contient également une liste de recommandations permettant de supprimer les vulnérabilités trouvées.

L'audit ne doit pas être confondu avec l'analyse de risques. Il ne permet *que* de trouver les vulnérabilités, mais pas de déterminer si celles-ci sont tolérables. Au contraire, l'analyse de risque permet de dire quels risques sont pris en compte, ou acceptés pour le SI. L'auditeur (le prestataire) dresse donc des recommandations, que l'audité (le client) suivra, ou ne suivra pas. Le client déterminera s'il suivra les recommandations ou non, en se référant à la politique de sécurité.

IV.7.2. Pratique de l'audit :

Pour arriver à dresser une liste la plus exhaustive possible des vulnérabilités d'un système, différentes pratiques existent et sont traditionnellement mises en œuvre.

- **Interviews :**

Les interviews sont généralement essentiels à tout audit. Dans le cas où l'organisation du SI est analysée, ils sont même indispensables. Toutes les personnes ayant un rôle à jouer dans la sécurité du SI sont à interroger :

- Le directeur des systèmes d'information (DSI)
- Le ou les responsable(s) de la sécurité des systèmes d'information (RSSI)
- Les administrateurs
- Les utilisateurs du système d'information, qu'ils aient un rôle dans la production de l'entreprise, dans la gestion, ou la simple utilisation des moyens informatiques
- Tout autre rôle ayant un lien avec la sécurité

Il est important de formuler les questions avec tact. En effet, interroger des personnes à propos de leur travail peut faire qu'elles se sentent jugées et les résultats peuvent être faussés. La diplomatie est donc une compétence essentielle pour la pratique des audits !

- **Les tests d'intrusion :**

Les tests d'intrusion sont une pratique d'audit technique. On peut diviser les tests d'intrusion en trois catégories principales : les tests *boîte blanche*, les tests *boîte grise* et les tests dits *boîte noire*. [18]

Un test *boîte noire* signifie que la personne effectuant le test se situe dans des conditions *réelles* d'une intrusion : le test est effectué de l'extérieur, et l'auditeur dispose d'un minimum d'informations sur le système d'information. Ce genre de tests débute donc par l'identification de la cible :

- Collecte d'informations publiques : pages web, informations sur les employés, entreprise ayant un lien de confiance avec la cible.
- Identification des points de présence sur internet.
- Ecoute du réseau.

Lors de la réalisation de tests *boîte grise*, l'auditeur dispose de quelques informations concernant le système audité. En général, on lui fournit un compte utilisateur. Ceci lui permet de se placer dans la peau d'un "utilisateur normal".

Les tests *boîte blanche* débutent avec toutes ces informations (et beaucoup plus) à disposition. Ensuite commence la recherche des vulnérabilités, à l'aide de différents tests techniques, comme par exemple la recherche des ports ouverts, la version des applications... Différents produits existent pour effectuer ces tests, et certains prévoient d'automatiser toute une batterie de tests (Nessus, LANguard...). [18]

La dernière phase est l'exploitation des vulnérabilités. Des effets indésirables pouvant survenir (déni de service par exemple), le côté pratique de cette phase n'est pas systématique. Elle consiste à déterminer les moyens à mettre en œuvre pour compromettre le système à l'aide des vulnérabilités découvertes. Selon les moyens à mettre en œuvre, le client pourra décider que le risque associé à la vulnérabilité décelée est négligeable (probabilité d'exploitation faible) ou au contraire à prendre en compte. Pour prouver la faisabilité de l'exploitation, les auditeurs créent des programmes qui exploitent la vulnérabilité, appelés exploits.

- **Les relevés de configuration :**

Il s'agit ici d'analyser, profondément, les composants du système d'information. Les configurations sont inspectées dans les moindres détails. Suite à cette observation, la liste des vulnérabilités est dégagée en comparant le relevé à des configurations réputées sécurisées , et à des ensembles de failles connues.

Tout peut être inspecté, allant de l'architecture du SI aux applications, en passant par les hôtes (clients et serveurs). Par exemple sur un serveur, on va analyser :

- le chargeur de démarrage,
- les mécanismes d'authentification (robustesse des mots de passe, utilisation d'authentification forte...),
- le système de fichiers (droits d'accès, utilisation de chiffrement...),
- les services
- la journalisation,
- la configuration réseau,
- ...

- **L'audit de code :**

Il existe des bases de vulnérabilités très fiables pour les applications répandues. Néanmoins, pour des applications moins utilisées, ou codées par l'entreprise elle-même, il peut être nécessaire d'analyser leur sécurité. Si les sources de l'application sont disponibles, il faut lire et comprendre le code source, pour déceler les problèmes qui peuvent exister. Notamment, les débordements de tampon (buffer overflow), les bugs de format, ou pour une application web, les vulnérabilités menant à des injections SQL...

L'audit de code est une pratique très fastidieuse et longue. De plus, elle ne permet généralement pas, en raison de la complexité, de dresser une liste exhaustive des vulnérabilités du code. Des méthodes automatiques existent, et permettent de *dégrossir* le travail, avec des outils comme RATS. Mais se reposer uniquement sur ce genre de méthodes peut nous faire passer à côté de problèmes flagrants pour un humain.

- **Fuzzing : test à données aléatoires :**

Pour les applications *boite noire*, où le code n'est pas disponible, il existe un pendant à l'analyse de code, qui est le fuzzing. Cette technique consiste à analyser le comportement d'une application en injectant en entrée des données plus ou moins aléatoires, avec des valeurs *limites*. Contrairement à l'audit de code qui est une analyse structurelle, le fuzzing est une analyse comportementale d'une application.

IV.7.3. Outils d'audit :

- **Référentiels :**

  - COBIT (Control objectives for information and technology ISACA) : propose un référentiel pour les systèmes d'information,
  - L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est la référence française en matière de SSI, et a produit notamment un référentiel général de sécurité (normes et recommandations).

IV.8. Classification des approches :

Une approche inspirée de meilleures pratiques permet d'espérer bénéficier de l'expérience, des succès et aussi des erreurs de pairs, qui ont déjà dû traiter les mêmes sujets. Pour une entreprise, cette approche lui permet également de se comparer aux pratiques vraisemblablement mises en œuvre par les autres, en espérant faire ce qu'il faut pour être en sécurité, sans en faire trop, et donc sans investir dans des mesures moins rentables [A9]. D'un autre côté, l'avantage des normes est d'être… des normes justement, qui constituent, enfin peut-on l'espérer, un consensus, voire au pire un compromis, entre experts internationaux sur la meilleure façon de traiter un sujet. Les meilleures pratiques et les normes abordent la plupart du temps la problématique de la SI avec des orientations différentes. Schématiquement, on peut classifier les approches possibles comme suit :

TABLEAU 1

Orientation de l'approche	Meilleures pratiques	Normes
Gestion des risques	EBIOS[1] MEHARI[2] OCTAVE[3]	
Processus	ITIL[6]	ISO 9001[4] ISO 13335-2, 13335-3[4] BS 7799-2[5]
Contrôles / Mesures de protection	COBIT[7] IT Baseline Protection Manual du BSI [8]	ISO 17799[4] ISO 13335-4
Produits		ISO 15408[4]

Figure 25 : Classification des approches

S'appuyer sur de telles approches, quelles qu'elles soient, permet de s'assurer d'une certaine exhaustivité, cohérence et homogénéité dans sa démarche, et fournit également des éléments

communs (vocabulaire, concepts, …) à tous les intervenants dans le projet : décideurs, utilisateurs, personnels de l'informatique, sous-traitants, fournisseurs, partenaires, etc. [19]

IV.8.1.Méthodes d'analyse de risques :

IV.8.1.1. Expression des besoins et identification des objectifs de sécurité :

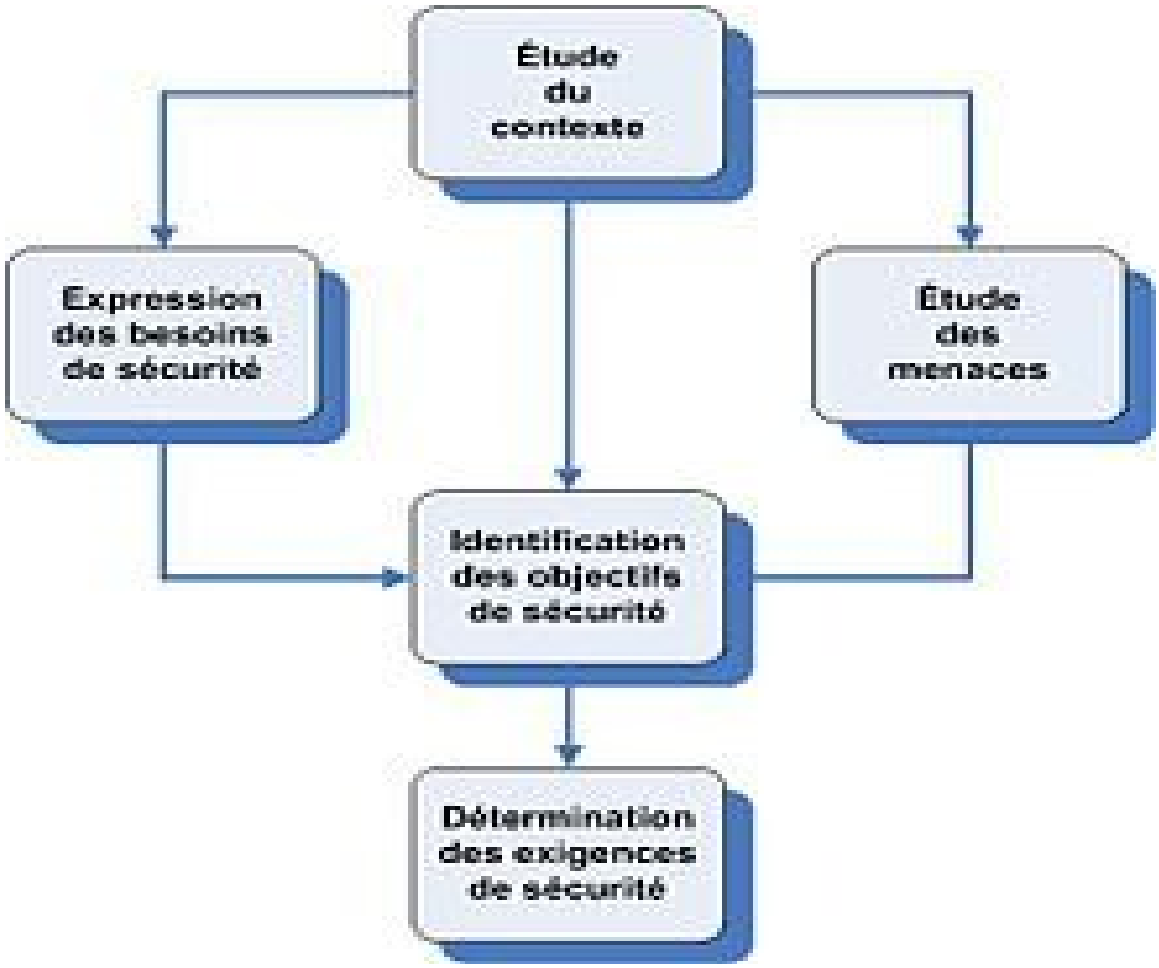


Figure 26: Schéma synthétique de la méthode EBIOS

La **méthode EBIOS** est une méthode d'évaluation des risques en informatique, développée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Elle permet d'apprécier les risques Sécurité des systèmes d'information (entités et vulnérabilités, méthodes d'attaques et éléments menaçants, éléments essentiels et besoins de sécurité...), de contribuer à leur traitement en spécifiant les exigences de sécurité à mettre en place, de préparer l'ensemble du dossier de sécurité nécessaire à l'acceptation des risques et de fournir les éléments utiles à la communication relative aux risques. Elle est compatible avec les normes ISO 13335 (GMITS), ISO 15408 (critères communs) et ISO 17799.

- **Utilisateurs :**

EBIOS est largement utilisée dans le secteur public (l'ensemble des ministères et des organismes sous tutelle), dans le secteur privé (cabinets de conseil, petites et grandes entreprises), en France et à l'étranger (Union européenne, Québec, Belgique, Tunisie, Luxembourg…), par de nombreux organismes en tant qu'utilisateurs ou bénéficiaires d'analyses de risques SSI.

- **Étapes de la démarche :**

EBIOS fournit une méthode permettant de construire une politique de sécurité en fonction d'une analyse des risques qui repose sur le contexte de l'entreprise et des vulnérabilités liées à son SI. La démarche est donc commune à tous, mais les résultats de chaque étape sont personnalisés. [1]

- **Étude du contexte :**

Cette étape essentielle a pour objectif d'identifier globalement le système-cible et de le situer dans son environnement. Elle permet notamment de préciser pour le système les enjeux, le contexte de son utilisation, les missions ou services qu'il doit rendre et les moyens utilisés.

L'étape se divise en trois activités:

- Étude de l'organisme : cette activité consiste à définir le cadre de l'étude. Il faut collecter les données concernant l'organisme et son système d'information.
- Étude du Système Cible : cette activité a pour but de préciser le contexte d'utilisation du système à concevoir ou existant.
- Détermination de la cible de l'étude de sécurité : cette activité a pour but de déterminer les entités sur lesquelles vont reposer les éléments essentiels du système-cible.

- **Expression des besoins :**

Cette étape contribue à l'estimation des risques et à la définition des critères de risques. Elle permet aux utilisateurs du système d'exprimer leurs besoins en matière de sécurité pour les fonctions et informations qu'ils manipulent. Ces besoins de sécurité s'expriment selon différents critères de sécurité tels que la disponibilité, l'intégrité et la confidentialité. L'expression des besoins repose sur l'élaboration et l'utilisation d'une échelle de besoins et la mise en évidence des impacts inacceptables pour l'organisme.

L'étape se divise en deux activités :

- Réalisation des fiches de besoins : cette activité a pour but de créer les tableaux nécessaires à l'expression des besoins de sécurité par les utilisateurs.
- Synthèse des besoins de sécurité : Cette activité a pour but d'attribuer à chaque élément essentiel des besoins de sécurité.

- **Étude des menaces :**

Cette étape consiste en un recensement des scénarios pouvant porter atteinte aux composants du SI. Une menace peut être caractérisée selon son type (naturel, humain ou environnemental) et/ou selon sa cause (accidentelle ou délibérée).

Ces menaces sont formalisées en identifiant leurs composants : les méthodes d'attaque auxquelles l'organisme est exposé, les éléments menaçants qui peuvent les employer, les vulnérabilités exploitables sur les entités du système et leur niveau.

- Étude des origines des menaces : Cette activité correspond à l'identification des sources dans le processus de gestion des risques.
- Étude des vulnérabilités : Cette activité a pour objet la détermination des vulnérabilités spécifiques du système-cible.
- Formalisation des menaces : À l'issue de cette activité, il sera possible de disposer d'une vision objective des menaces pesant sur le système-cible.

➢ **Identification des objectifs de sécurité :**

Un élément menaçant peut affecter des éléments essentiels en exploitant les vulnérabilités des entités sur lesquelles ils reposent avec une méthode d'attaque particulière. Les objectifs de sécurité consistent à couvrir les vulnérabilités.

- Confrontation des menaces aux besoins de sécurité : cette confrontation permet de retenir et hiérarchiser les risques qui sont véritablement susceptibles de porter atteinte aux éléments essentiels.
- Formalisation des objectifs de sécurité : Cette activité a pour but de déterminer les objectifs de sécurité permettant de couvrir les risques.
- Détermination des niveaux de sécurité : Cette activité sert à déterminer le niveau de résistance adéquat pour les objectifs de sécurité. Elle permet également de choisir le niveau des exigences de sécurité d'assurance.

➢ **Détermination des exigences de sécurité :**

L'équipe de mise en œuvre de la démarche doit spécifier les fonctionnalités de sécurité attendues. L'équipe chargée de la mise en œuvre de la démarche doit alors démontrer la parfaite couverture des objectifs de sécurité par les exigences fonctionnelles et les exigences d'assurance.

➢ **Avantages et Inconvénients :**

❖ **Avantages :**

- Une méthode claire : elle définit clairement les acteurs, leurs rôles et les interactions.
- Une approche exhaustive : contrairement aux approches d'analyse des risques par scénarios, la démarche structurée de la méthode EBIOS permet d'identifier les éléments constitutifs des risques.
- Une démarche adaptative : la méthode EBIOS peut être adaptée au contexte de chacun et ajustée à ses outils et habitudes méthodologiques grâce à une certaine flexibilité.

❖ **Inconvénients :**

- La méthode EBIOS ne fournit pas de recommandations ni de solutions immédiates aux problèmes de sécurité.
- Il n'y a pas d'audit et d'évaluation de la méthode.

IV.8.1.2. Méthode d'analyse de risques informatiques optimisée par niveau :

La **méthode d'analyse de risques informatiques orientée par niveau** (**Marion**) est une méthode d'audit, proposée depuis 1983 par le CLUSIF, visant à évaluer le niveau de sécurité informatique d'une entreprise. L'objectif est double :

1. situer l'entreprise auditée par rapport à un niveau jugé correct, et par rapport au niveau atteint par les entreprises similaires
2. identifier les menaces et vulnérabilités à contrer.

- **Principe :**
- **Six thèmes :**

L'analyse est articulée en 6 grands thèmes:

1. la sécurité organisationnelle
2. la sécurité physique
3. la continuité de service
4. l'organisation informatique
5. la sécurité logique et l'exploitation
6. la sécurité des applications

- **Vingt-sept indicateurs :**

Les indicateurs, répartis dans ces 6 thèmes, vont être évalués, et valorisés sur une échelle de 0 (très insatisfaisant) à 4 (très satisfaisant), le niveau 3 étant le niveau jugé correct. Chaque indicateur est affecté d'un poids en fonction de son importance.

- **Dix-sept types de menaces :**

1. Accidents physiques
2. Malveillance physique
3. Panne du SI
4. Carence de personnel
5. Carence de prestataire
6. Interruption de fonctionnement du réseau
7. Erreur de saisie
8. Erreur de transmission
9. Erreur d'exploitation
10. Erreur de conception / développement
11. Vice caché d'un progiciel
12. Détournement de fonds
13. Détournement de biens
14. Copie illicite de logiciels
15. Indiscrétion / détournement d'information
16. Sabotage immatériel
17. Attaque logique du réseau

- **Phases :**
  - **Préparation :**

- Les objectifs de sécurité de l'entreprise sont définis

- Le champ d'action de l'analyse est défini, ainsi que le découpage fonctionnel de ce champ d'action

❖ **Audit des vulnérabilités :**

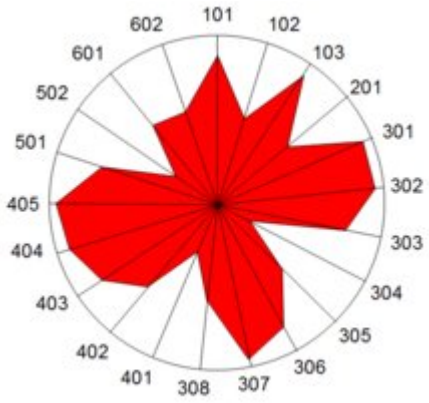


Figure 27 : Exemple de rosace réalisée dans le cadre de la méthode MARION

Cette phase se base sur les questionnaires fournis par la méthode

- Les contraintes de l'entreprise sont identifiées.
- Les indicateurs sont valorisés de 0 à 4. Chaque indicateur est affecté d'un poids relatif.
- L'ensemble des indicateurs est très souvent représenté sous forme graphique : rosace/radar, diagramme en barres, ... Des diagrammes de synthèse sont également possibles : rosace par source des risques (accident, malveillance, erreur), par impact des risques (disponibilité, intégrité, confidentialité des informations), ... [19]

❖ **Analyse des risques :**

- L'exploitation des résultats de l'audit permet de répartir les risques en *majeurs* (RM) et *simples* (RS).
- Le SI est alors découpé en fonctions. Les groupes fonctionnels spécifiques hiérarchisés selon l'impact et la potentialité des risques les concernant sont identifiés. Pour chaque groupe fonctionnel de l'entreprise, chaque fonction est revue en détail afin d'évaluer les scénarios d'attaque possibles avec leur impact et leur potentialité. Voir ci-dessus la typologie des menaces proposée par la méthode.

❖ **Élaboration du plan d'action :**

- Les menaces et vulnérabilités qui pèsent sur l'entreprise étant identifiées et valorisées, l'entreprise décide du degré d'amélioration à apporter pour réduire ces risques et idéalement atteindre la note globale de 3.
- Elle définit les moyens à y affecter. On évalue le coût de la mise en conformité.
- Les tâches sont décrites et ordonnancées.

IV.8.1.3. Méthode harmonisée d'analyse des risques :

La **méthode harmonisée d'analyse des risques** (**MEHARI**) est une méthode visant à la sécurisation informatique d'une entreprise ou d'un organisme. Elle a été développée et est proposée par le CLUSIF.

Le CLUSIF a présenté le 27 janvier 2010 une nouvelle version de sa méthode MEHARI.

- **Objectifs :**

- différencier les modes de mise en œuvre des services de sécurité ;
- limiter le volume de travail à fournir pour l'étude.

Découpage en objectifs :

- base unique d'appréciation de la sécurité ;
- délégation des décisions ;
- équilibre des moyens et cohérence des contrôles.

- **Concepts :**

  - **Séparation en cellules :**

MEHARI propose 8 types de cellules :

- l'entité ;
- le site ;
- les locaux ;
- les applicatifs ;
- les services offerts par les systèmes et l'infrastructure ;
- le développement ;
- la production informatique ;
- les réseaux et les télécoms.

  - **Scénarios de sinistre :**

Les risques sont classés selon le type de leur cible. Chaque scénario doit avoir :

- une seule cause : erreur, malveillance, accident ;
- une seule conséquence : atteinte à la disponibilité, intégrité, confidentialité.

  - ***Méthodes de résolution :***

- Combattre les agressions.
  - connaître les menaces, les vulnérabilités ;
  - connaitre la source (interne ou externe)
  - imaginer les agressions ;
- Élaborer des mesures à mettre en place : évaluer l'efficacité, évaluer la robustesse ;
- Recours possible : transfert sur un tiers —l'assurance, le responsable de l'attaque.

✓ ***Impact :***

L'impact est l'ampleur des conséquences de la survenue d'un événement possible.

- L'impact des *détériorations* peut être réduit par des *mesures de protection*.
- L'impact des *dysfonctionnements* peut être réduit par des *mesures palliatives*.
- L'impact des *pertes finales* peut être réduit par des *mesures de récupération*.

L'impact, fonction de ces trois critères, est évalué de 1 (faible) à 4 (grave).

✓ ***Potentialité :***

La potentialité est la probabilité qu'un événement possible survienne effectivement. Elle peut être due à :

- une *exposition naturelle* : elle peut être diminuée par des *mesures structurelles* ;
- une *intention d'agression* : elle peut être diminuée par des *mesures dissuasives* ;
- des *possibilités de sinistre* : elle peut être diminuée par des *mesures préventives*.

Elle est mesurée de 0 (nulle) à 4 (forte).

❖ **Gravité :**

La gravité est fonction, et non le produit, de l'impact et de la potentialité. Sa valeur en fonction de ces deux facteurs s'obtient par une grille (table), qui doit être personnalisée par l'entreprise qui applique la méthode.

➢ **Démarche :**

- Découpage en cellules
- Échelles de valeurs et objectifs de sécurité compris
- Classification exhaustive des ressources
- Scénarios représentatifs des risques
- Participation active des intéressés

IV.8.2. Normes de sécurité :

IV.8.2.1. ISO 13335 :

La norme **ISO 13335** est une norme de sécurité des systèmes d'information.

Cette norme est actuellement rédigée en anglais et n'a pas été traduite en français.

Elle trouve son origine dans quatre documents (rapports techniques) considérés comme des références :

1. Définitions et concepts de base,
2. Informations sur l'organisation à prévoir dans toute entreprise,
3. Approches de gestion du risque,
4. Guide de choix des mesures préventives selon les circonstances de l'environnement.

La norme se décompose en quatre parties :

- ISO 13335-1 : Concepts et modèles pour la gestion de la sécurité des technologies de l'information et de la communication (2004).
- ISO 13335-3 : Techniques pour la gestion de la sécurité informatique (1998).
- ISO 13335-4 : Sélection de sauvegardes (2000).
- ISO 13335-5 : Guide pour la gestion de sécurité du réseau (2001). [17]

IV.8.2.2. ISO/CEI 17799 :

La norme **ISO/CEI 17799** est une norme internationale concernant la sécurité de l'information, publiée en décembre 2000 par l'ISO dont le titre est *Code de bonnes pratiques pour la gestion de la sécurité d'information*. [A10]

La deuxième édition de cette norme a été publiée en juin 2005, elle comporte un nouveau chapitre : "Analyse des risques". Cette deuxième édition a changé de numéro de référence en juillet 2007. Il s'agit maintenant de la norme **ISO/CEI 27002**.

IV.8.2.3. ISO/CEI 27001 :

L'**ISO/CEI 27001** est une norme internationale de système de gestion de la sécurité de l'information, publiée en octobre 2005 par l'ISO dont le titre est *Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences*.[A10]

- **Objectifs :**

La norme ISO 27001 publiée en octobre 2005 et révisée en 2013 succède à la norme BS 7799-2 de BSI (*British Standards Institution*). Elle s'adresse à tous les types d'organismes (entreprises commerciales, ONG, administrations…) La norme ISO/CEI 27001 décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI). Le SMSI est destiné à choisir les mesures de sécurité afin d'assurer la protection des biens sensibles d'une entreprise sur un périmètre défini.

L'ISO/CEI 27001 définit l'ensemble des contrôles à effectuer pour s'assurer de la pertinence du SMSI, à l'exploiter et à le faire évoluer. Plus précisément, l'annexe A de la norme est composée des 114 mesures de sécurité de la norme ISO/CEI 27002 (anciennement ISO/CEI 17799), classées dans 14 sections. Comme pour les normes ISO 9001 et ISO 14001, il est possible de se faire certifier ISO 27001.

La version 2013 ne fait plus explicitement allusion au PDCA (ou roue de Deming), elle utilise la formulation « établir, implémenter, maintenir, améliorer ».

- **La structure de la norme**

La norme 27001 comporte 11 chapitres ; les exigences qu'ils contiennent doivent obligatoirement être respectées pour répondre à cette norme et obtenir une certification.

- **Phase Plan :**

Fixe les objectifs du SMSI. La phase Plan du SMSI comprend 4 étapes :

Étape 1 : Définir la politique et le périmètre du SMSI

Périmètre : domaine d'application du SMSI. Son choix est libre, mais il doit être bien défini, car il doit comprendre toutes les activités pour lesquelles les parties prenantes exigent de la confiance.

Politique : niveau de sécurité (intégrité, confidentialité, disponibilité de l'information) qui sera pratiqué au sein de l'entreprise. La norme n'impose pas de niveau minimum de sécurité à atteindre dans le SMSI.

Le choix du périmètre et de la politique étant libre, ces deux éléments sont des « leviers de souveraineté » pour l'entreprise. Ainsi, une entreprise peut être certifiée ISO 27001 tout en définissant un périmètre très réduit et une politique de sécurité peu stricte et sans répondre aux exigences de ses clients en termes de sécurité.

Étape 2 : Identifier et évaluer les risques liés à la sécurité et élaborer la politique de sécurité

La norme ISO 27001 ne donne pas de directives sur la méthode d'appréciation des risques à adopter. Les entreprises peuvent donc en inventer une en veillant à bien respecter le cahier des charges ou en choisir une parmi les plus courantes notamment la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) mise en place en France par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Le cahier des charges relatif à l'appréciation des risques se développe en 7 points :

1. Identifier les actifs.
2. Identifier les personnes responsables.
3. Identifier les vulnérabilités.
4. Identifier les menaces.
5. Identifier les impacts.
6. Évaluer la vraisemblance.
7. Estimer les niveaux de risque.

Étape 3 : Traiter le risque et identifier le risque résiduel par un plan de gestion

Il existe 4 traitements possibles de chacun des risques identifiés :

1. L'acceptation : ne mettre en place aucune mesure de sécurité supplémentaire car les conséquences de cette attaque sont faibles (exemple : vol d'un ordinateur portable ne comportant pas de données primordiales pour l'entreprise, piratage de la vitrine web…) Cette solution ne doit être que ponctuelle pour éviter la perte de confiance des parties prenantes.
2. L'évitement : politique mise en place si l'incident est jugé inacceptable.
3. Le transfert : lorsque le risque ne peut pas être évité et qu'elle ne peut pas mettre en place les mesures de sécurité nécessaires elle transfère le risque par le biais de la souscription d'une assurance ou de l'appel à la sous-traitance.
4. La réduction : le rendre à un niveau acceptable par la mise en œuvre de mesures techniques et organisationnelles, solution la plus utilisée.

Lorsque la décision de traitement du risque est prise l'entreprise doit identifier les risques résiduels c'est-à-dire ceux qui persistent après la mise en place des mesures de sécurité. S'ils sont jugés inacceptables, il faut définir des mesures de sécurité supplémentaires.

Étape 4 : Choisir les mesures de sécurité à mettre en place

La norme ISO 27001 dispose d'une annexe A qui propose 114 mesures de sécurité classées en 14 catégories (politique de sécurité, sécurité du personnel, contrôle des accès… Cette annexe normative est qu'une liste qui ne donne aucun conseil de mise en œuvre au sein de l'entreprise.

- **Phase Do :**

Met en place les objectifs

Elle se découpe en plusieurs étapes :

1. Établir un plan de traitement des risques.
2. Déployer les mesures de sécurité.
3. Générer des indicateurs
    - De performance pour savoir si les mesures de sécurité sont efficaces.
    - De conformité qui permettent de savoir si le SMSI est conforme à ses spécifications.
4. Former et sensibiliser le personnel.

- **Phase Check :**

Consiste à gérer le SMSI au quotidien et à détecter les incidents en permanence pour y réagir rapidement 3 outils peuvent être mis en place pour détecter ces incidents :

1. Les audits internes qui vérifient la conformité et l'efficacité du système de management. Ces audits sont ponctuels et planifiés.
2. Le contrôle interne qui consiste à s'assurer en permanence que les processus fonctionnent normalement.
3. Les revues (ou réexamens) qui garantissent l'adéquation du SMSI avec son environnement.

- **Phase Act :**

Mettre en place des actions correctives, préventives ou d'amélioration pour les incidents et écarts constatés lors de la phase *Check*.

- Actions correctives : agir sur les effets pour corriger les écarts puis sur les causes pour éviter que les incidents ne se reproduisent.
- Actions préventives : agir sur les causes avant que l'incident ne se produise.
- Actions d'amélioration : améliorer la performance d'un processus du SMSI.

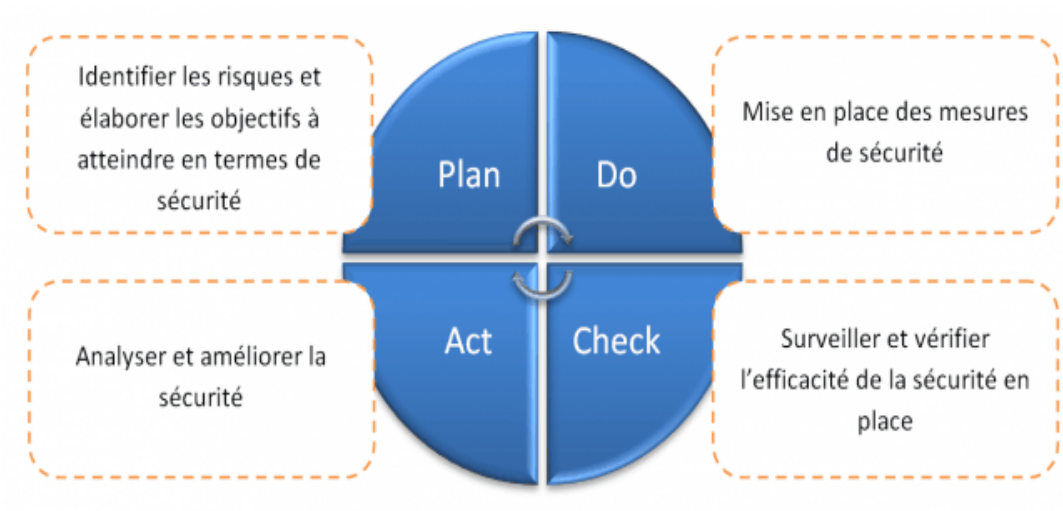


Figure 28 :Les quatre phases PDCA:

- **Processus de certification :**

La certification n'est pas un but en soi, c'est-à-dire que l'organisme qui décide de mettre en place un SMSI en suivant les exigences de l'ISO 27001, n'a pas pour obligation de se faire certifier. Cependant, c'est l'aboutissement logique de l'implémentation d'un SMSI puisque les parties prenantes n'ont confiance qu'en un système certifié par un organisme indépendant.

L'obtention du certificat ISO 27001 passe par trois audits : l'audit initial, l'audit de surveillance et l'audit de renouvellement.

L'audit initial porte sur l'ensemble du SMSI. Sa durée est déterminée dans l'annexe C de la norme ISO 27006. L'auditeur ne donne pas la certification, il donne juste un avis qui sera étudié par un comité de validation technique, puis par un comité de certification. Ce n'est qu'après cela qu'elle obtient le certificat pour une durée de trois ans. Dans le cas contraire, il y a un audit complémentaire dans le délai maximum de trois mois. L'organisme devra durant ce délai corriger les problèmes décelés lors de l'audit initial pour obtenir le certificat.

L'audit de surveillance a lieu pendant la période de validité du certificat (3 ans) afin de s'assurer que le SMSI est toujours valable. Il y en a un par an. L'audit porte sur les non-conformités relevées lors de l'audit initial ainsi que sur d'autres points :

- Le traitement des plaintes.
- L'état d'avancement des activités planifiées.
- L'utilisation de la marque de l'organisation certificatrice.
- La viabilité du SMSI.
- Différentes clauses choisies par l'auditeur.

Si l'auditeur relève des non-conformités, le certificat sera suspendu voire annulé. L'entreprise doit donc être perpétuellement mobilisée.

L'audit de renouvellement se déroule à l'échéance du certificat. Il porte sur les non-conformités du dernier audit de surveillance ainsi que sur la revue des rapports des audits de surveillance précédents et la revue des performances du SMSI sur la période.

- **Critique du standard :**

***Avantages* :**

- Une description pratique et détaillée de la mise en œuvre des objectifs et mesures de sécurité.
- Un audit régulier qui permet le suivi entre les risques initialement identifiés, les mesures prises et les risques nouveaux ou mis à jour, afin de mesurer l'efficacité des mesures prises.
- Sécurité :

1. Processus d'amélioration continue de la sécurité, donc le niveau de sécurité a plutôt tendance à croître.
2. Meilleure maîtrise des risques.
3. Diminution de l'usage des mesures de sécurité qui ne servent pas.

- Une certification qui améliore la confiance avec les parties prenantes.
- Homogénéisation : c'est un référentiel international. Cela facilite les échanges, surtout pour les entreprises qui possèdent plusieurs sites.
- Processus simple et peu coûteux : réduction des coûts grâce à la diminution d'usage de mesures de sécurité inutiles et à la mutualisation des audits (baisse du nombre et de la durée des audits quand on obtient la certification).
- La norme fournit des indicateurs clairs et fiables ainsi que des éléments de pilotage financier aux directions générales.
- La norme permet d'identifier plus efficacement les risques et les coûts associés.

***Limites* :**

- Parfois, faible expérience des organismes d'accréditation par rapport aux spécificités des enjeux en sécurité des systèmes d'information.
- Relations commerciales prépondérantes (achat de certification, de conseil, de produits, de services), ce qui conduit à une dévalorisation du processus d'accréditation.
- Durée courte pour les audits.
- La définition et la mise en place d'une méthodologie sont des tâches lourdes.
- L'application de cette norme ne réduit pas forcément de manière notable le risque en matière de piratage et de vols d'informations confidentielles. Les intervenants, notamment internes, connaissent les règles et peuvent ainsi plus aisément les contourner. Les normes sont inopérantes dans ce domaine.

IV.8.2.4.ISO/CEI 27002 :

La norme **ISO/CEI 27002** est une norme internationale concernant la sécurité de l'information, publiée en 2005 par l'ISO, dont le titre en français est *Code de bonnes pratiques pour la gestion de la sécurité de l'information.*

L'ISO/CEI 27002 est un ensemble de 133 mesures dites « best practices » (bonnes pratiques en français), destinées à être utilisées par tous ceux qui sont responsables de la mise en place ou du maintien d'un Système de Management de la Sécurité de l'Information (SMSI). La sécurité de l'information est définie au sein de la norme comme la « préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information ». [1]

Cette norme n'a pas de caractère obligatoire pour les entreprises. Son respect peut toutefois être mentionné dans un contrat : un prestataire de services pourrait ainsi s'engager à respecter les pratiques normalisées dans ses relations avec un client.

- **Objectifs :**

ISO/IEC 27002 est plus un code de pratique, qu'une véritable norme ou qu'une spécification formelle telle que l'ISO/IEC 27001. Elle présente une série de contrôles (39 objectifs de contrôle) qui suggèrent de tenir compte des risques de sécurité des informations relatives à la confidentialité, l'intégrité et les aspects de disponibilité. Les entreprises qui adoptent l'ISO/CEI 27002 doivent évaluer leurs propres risques de sécurité de l'information et appliquer les contrôles appropriés, en utilisant la norme pour orienter l'entreprise. [17]

La norme ISO 27002 n'est pas une norme au sens habituel du terme. En effet, ce n'est pas une norme de nature technique, technologique ou orientée produit, ou une méthodologie d'évaluation d'équipement telle que les critères communs CC/ISO 15408. Elle n'a pas de caractère d'obligation, elle n'amène pas de certification, ce domaine étant couvert par la norme ISO/IEC 27001.

- **Mise en œuvre :**

La norme ne fixe pas de niveaux ou d'objectifs de sécurité et rappelle dans les chapitres d'introduction, la nécessité de faire des analyses de risques périodiques mais ne précise aucune obligation quant à la méthode d'évaluation du risque, il suffit donc de choisir celle qui répond aux besoins. C'est à partir des résultats de l'analyse de risque que l'organisation « pioche » dans les différentes rubriques de la norme celles qu'elle doit mettre en œuvre pour répondre à ses besoins de sécurité. En 2002, plus de 80 000 entreprises [17] se conformaient à cette norme à travers le monde.

- **Contenu de la norme :**

La norme ISO/CEI 27002 est composé de 15 chapitres dont 4 premiers introduisent la norme et les 11 chapitres suivants couvrent le management de la sécurité aussi bien dans ses aspects stratégiques que dans ses aspects opérationnels.

Chapitre n° 1 : Champ d'application

La norme donne des recommandations pour la gestion de la sécurité des informations pour ceux qui sont chargés de concevoir, mettre en œuvre ou maintenir la sécurité.

Chapitre n° 2 : Termes et définitions

« Sécurité de l'information » est explicitement définie comme la «préservation de la confidentialité, l'intégrité et la disponibilité de l'information». Ceux-ci et d'autres termes connexes sont définies plus loin.

Chapitre n° 3 : Structure de la présente norme

Cette page explique que la norme contient des objectifs de contrôle.

Chapitre n° 4 : Évaluation des risques et de traitement

ISO / CEI 27002 couvre le sujet de la gestion des risques. Elle donne des directives générales sur la sélection et l'utilisation de méthodes appropriées pour analyser les risques pour la sécurité des informations ; elle ne prescrit pas une méthode spécifique, puisque celle-ci doit être appropriée selon le contexte.

Chapitre n° 5 : Politique de sécurité de l'information

Il mentionne la nécessité pour l'organisme de disposer d'une politique de sécurité de l'information et de la réexaminer régulièrement.

Chapitre n° 6 : Organisation de la sécurité de l'information

Il décrit les mesures nécessaires pour l'établissement d'un cadre de gestion de la sécurité en interne et traite de tous les aspects contractuels liés à la sécurisation de l'accès par des tiers (clients, sous-traitants, …) au système d'information.

Chapitre n° 7 : Gestion des actifs

Il montre l'importance d'inventorier et de classifier les actifs de l'organisme afin de maintenir un niveau de protection adapté. Ces actifs peuvent être :

- des biens physiques (serveurs, réseau, imprimantes, baies de stockage, poste de travail, des matériels non IT),
- des informations (base de données, fichiers, archives),
- des logiciels (application ou système),
- des services,
- de la documentation (politiques, procédures, plans).

Chapitre n° 8 : Sécurité liée aux ressources humaines

Il donne les recommandations destinées à réduire le risque d'erreur ou de fraude en favorisant la formation et la sensibilisation des utilisateurs sur les risques et les menaces pesant sur les informations.

Chapitre n° 9 : Sécurités physiques et environnementales

Il décrit les mesures pour protéger les locaux de l'organisme contre les accès non autorisés et les menaces extérieures et environnementales ainsi que protéger les matériels (emplacement, maintenance, alimentation électrique …).

Chapitre n° 10 : Exploitation et gestion des communications

Il décrit les mesures permettant :

- d'assurer une exploitation correcte et sécurisée des moyens de traitement de l'information ;
- de gérer les prestations de service assurées par des tiers ;
- de réduire les risques de panne ;

- de protéger l'intégrité des informations et des logiciels ;
- de maintenir l'intégrité, la confidentialité et la disponibilité des informations et des moyens de traitement de l'information ;
- d'assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle ils s'appuient ;
- de maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité extérieure ;
- et enfin de détecter les traitements non autorisés de l'information.

Chapitre n° 11 : Contrôle d'accès

Il décrit les mesures pour gérer et contrôler les accès logiques aux informations, pour assurer la protection des systèmes en réseau, et pour détecter les activités non autorisées. Ce thème couvre aussi la sécurité de l'information lors de l'utilisation d'appareils informatiques mobiles et d'équipements de télétravail.

Chapitre n° 12 : Acquisition, développement et maintenance des systèmes d'informations

Il propose les mesures pour veiller à ce que la sécurité fasse partie intégrante des systèmes d'information. Ce thème traite aussi des mesures visant à prévenir la perte, la modification ou la mauvaise utilisation des informations dans les systèmes d'exploitation et les logiciels d'application et enfin à protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques.

Chapitre n° 13 : Gestion des incidents

Il souligne la nécessité de mettre en place des procédures pour la détection et le traitement des incidents de sécurité.

Chapitre n° 14 : Gestion de la continuité d'activité.

Il décrit des mesures pour la gestion d'un plan de continuité de l'activité visant à réduire le plus possible l'impact sur l'organisme et à récupérer les actifs informationnels perdus notamment à la suite de catastrophes naturelles, d'accidents, de pannes de matériel et d'actes délibérés.

Chapitre n° 15 : Conformité

Il traite :

- du respect des lois et des réglementations ;
- de la conformité des procédures en place au regard de la politique de sécurité
- et enfin de l'efficacité des dispositifs de traçabilité et de suivi des procédures, notamment les journaux d'activités, les audits et les enregistrements de transactions.

Cette norme est de plus en plus utilisée par les entreprises du secteur privé comme un référentiel d'audit et de contrôle, en complément de la politique de sécurité de l'information de l'entreprise. Le fait de respecter cette norme permet de viser, à moyen terme, la mise en place

d'un Système de Management de la Sécurité de l'Information, et à long terme, une éventuelle certification ISO/CEI 27001.

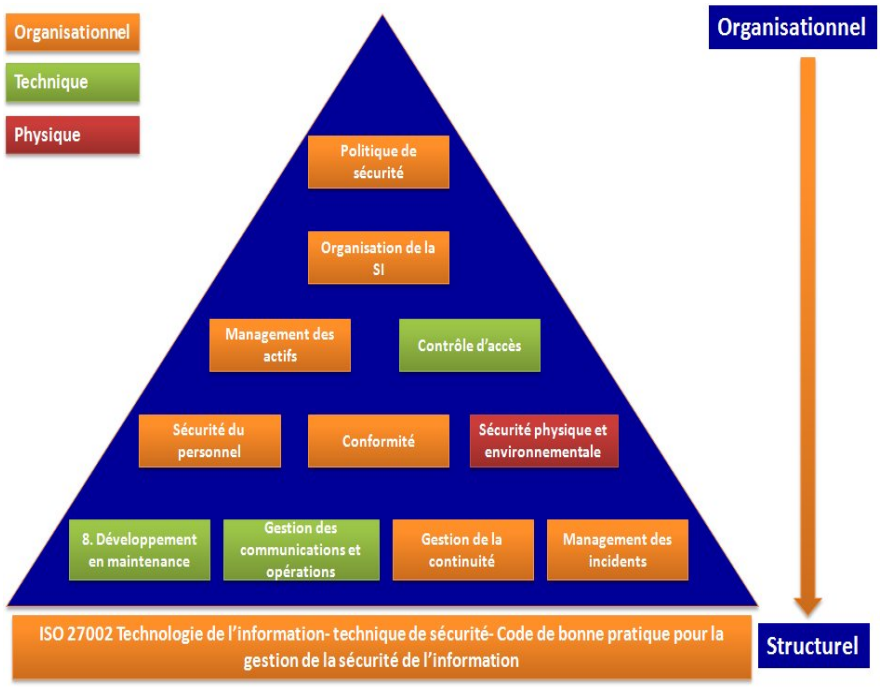


Figure 29 : Structure de l'ISO 27002

IV.8.2.5. ISO/CEI 27005 :

L'ISO (Organisation internationale de normalisation) a publié, le 4 juin 2008, la première norme de gestion des risques de la Sécurité des Systèmes d'Information : l'ISO/CEI 27005:2008. Cette norme est un standard international qui décrit le Système de Management des risques liés à la Sécurité de l'information.

Elle a été révisée le 19 mai 2011.

La norme ISO 27005 explique en détail comment conduire l'appréciation des risques et le traitement des risques, dans le cadre de la sécurité de l'information. La norme ISO 27005 propose une méthodologie de gestion des risques en matière d'information dans l'entreprise conforme à la norme ISO/CEI 27001. La nouvelle norme a donc pour but d'aider à mettre en œuvre l'ISO/CEI 27001, la norme relative aux systèmes de management de la sécurité de l'information (SMSI), qui est fondée sur une approche de gestion du risque. Néanmoins, la norme ISO 27005 peut être utilisée de manière autonome dans différentes situations. La norme ISO 27005 applique à la gestion de risques le cycle d'amélioration continue PDCA (Plan, Do, Check, Act) utilisé dans toutes les normes de systèmes de management. [2]

- PLAN : Identification des risques, évaluation des risques et définition des actions de réduction des risques.
- DO : Exécution de ces actions.
- CHECK : Contrôle du résultat.
- ACT : Modification du traitement des risques selon les résultats.

- **Contenu de la norme**

La norme ISO 27005 détaille le processus de gestion de risque dans les chapitres 6 à 12. Elle est complétée de 6 annexes de référence A à F, nécessaires à la mise en œuvre de la méthode.

- Chapitre 6 : le processus de gestion de risque est expliqué dans son ensemble.
- Chapitre 7 : établir le contexte de l'analyse des risques.
- Chapitre 8 : définition de l'appréciation des risques.
- Chapitre 9 : quatre choix du traitement du risque sont proposés.
- Chapitre 10 : acceptation du risque.
- Chapitre 11 : communication du risque.
- Chapitre 12 : surveillance et réexamen des risques.

IV.8.2.6. ISO/CEI 27006 :

ISO/CEI 27006 est un standard de sécurité de l'information publié conjointement par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI, ou IEC en anglais), faisant partie de la suite ISO/CEI 27000.

Son titre anglais est *IT Security techniques: Requirements for bodies providing audit and certification of Information Security Management Systems (ISMS).*

Son objet est de fournir les pré-requis pour les organismes d'audit et de certification à la norme ISO 27001 pour les Systèmes de Management de la Sécurité de l'Information. Cette norme a été remise à jour en 2011 et porte la référence ISO/IEC 27006:2011.

IV.9. Plan de continuité d'activité :

Un **plan de continuité d'activité**, a pour but de garantir la survie de l'entreprise après un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données. Ce plan est un des points essentiels de la politique de sécurité informatique d'une entreprise.

IV.9.1. Étapes de la mise en place d'un plan de continuité :

IV.9.1.1. Analyse de risque et d'impact :

Pour qu'un plan de continuité soit réellement adapté aux exigences de l'entreprise, il doit reposer sur une analyse de risque et une analyse d'impact :

- **L'analyse de risque** débute par une identification des menaces sur l'informatique. Les menaces peuvent être d'origine humaine (attaque délibérée ou maladresse) ou d'origine « naturelle » ; elles peuvent être internes à l'entreprise ou externes. On déduit ensuite le risque qui découle des menaces identifiées ; on mesure l'impact possible de ces risques. Enfin, on décide de mettre en œuvre des mesures d'atténuation des risques en se concentrant sur ceux qui ont un impact significatif [20]. Par exemple, si le risque de panne d'un équipement risque de tout paralyser, on installe un équipement redondant. Les mesures d'atténuation de risque qui sont mises en œuvre diminuent le niveau de risque, mais elles ne l'annulent pas : il subsiste toujours un

risque résiduel, qui sera couvert soit par le plan de continuité, soit par d'autres moyens (assurance, voire acceptation du risque).

- **L'analyse d'impact** consiste à évaluer quel est l'impact d'un risque qui se matérialise et à déterminer à partir de quand cet impact est intolérable, généralement parce qu'il met en danger les processus essentiels (donc, la survie) de l'entreprise. L'analyse d'impact se fait sur base de désastres : on considère des désastres extrêmes, voire improbables (par exemple, la destruction totale du bâtiment) et on détermine les impacts financiers, humains, légaux, etc., pour des durées d'interruption de plus en plus longues jusqu'à ce qu'on atteigne l'impact maximal tolérable [20]. Le résultat principal de l'analyse d'impact est donc une donnée temporelle : c'est la durée maximale admissible d'une interruption de chaque processus de l'entreprise. En tenant compte des ressources informatiques (réseaux, serveurs, PCs…) dont chaque processus dépend, on peut en déduire le temps maximal d'indisponibilité de chacune de ces ressources, en d'autres termes, le temps maximal après lequel une ressource informatique doit avoir été remise en fonction.

Une analyse de risque réussie est le résultat d'une action collective impliquant tous les acteurs du système d'information : techniciens, utilisateurs et managers.

IV.9.1.2. Choix de la stratégie de sécurisation :

Il existe plusieurs méthodes pour assurer la continuité de service d'un système d'information. Certaines sont techniques (choix des outils, méthodes de protection d'accès et de sauvegarde des données), d'autres reposent sur le comportement individuel des utilisateurs (extinction des postes informatiques après usage, utilisation raisonnable des capacités de transfert d'informations, respect des mesures de sécurité), sur des règles et connaissances collectives (protection incendie, sécurité d'accès aux locaux, connaissance de l'organisation informatique interne de l'entreprise) et de plus en plus sur des conventions passées avec des prestataires (copie des programmes, mise à disposition de matériel de secours, assistance au dépannage).

Les méthodes se distinguent entre **préventives** (éviter la discontinuité) et **curatives** (rétablir la continuité après un sinistre). Les méthodes préventives sont souvent privilégiées, mais décrire les méthodes curatives est une nécessité car aucun système n'est fiable à 100 %.

- **Mesures préventives :**

  - ✓ **La sauvegarde des données :**

La préservation des données passe par des copies de sauvegarde régulières. Il est important de ne pas stocker ces copies de sauvegarde à côté du matériel informatique, voire dans la même pièce car elles disparaitraient en même temps que les données à sauvegarder en cas d'incendie, de dégât des eaux, de vol, etc. Lorsqu'il est probable que les sauvegardes disparaissent avec le matériel, le stockage des copies de sauvegarde peut alors être nécessaire dans un autre lieu différent et distant.

L'analyse d'impact a fourni des exigences exprimées en temps maximal de rétablissement des ressources après un désastre (RTO: *Recovery Time Objective* ou Durée maximale d'interruption admissible) et la perte maximale de données (RPO *Recovery Point Objective* ou

Perte de données maximale admissible). La stratégie doit garantir que ces exigences seront observées.

- ✓ **Les systèmes de secours :**

Il s'agit de disposer d'un système informatique équivalent à celui pour lequel on veut limiter l'indisponibilité : ordinateurs, périphériques, systèmes d'exploitation, programmes particuliers, etc. Une des solutions consiste à créer et maintenir un **site de secours**, contenant un système en ordre de marche capable de prendre le relais du système défaillant. Selon que le système de secours sera implanté sur le site d'exploitation ou sur un lieu géographiquement différent, on parlera d'un secours *in situ* ou d'un secours *déporté*.

Pour répondre aux problématiques de recouvrement de désastre, on utilise de plus en plus fréquemment des sites délocalisés, c'est-à-dire physiquement séparés des utilisateurs, de quelques centaines de mètres à plusieurs centaines de kilomètres : plus le site est éloigné, moins il risque d'être touché par un désastre affectant le site de production. Mais la solution est d'autant plus chère, car la bande passante qui permet de transférer des données d'un site vers l'autre est alors généralement plus coûteuse et risque d'être moins performante. Cependant la généralisation des réseaux longues distances et la baisse des coûts de transmission rendent moins contraignante la notion de distance : le coût du site ou la compétence des opérateurs (leur capacité à démarrer le secours rapidement et rendre l'accès aux utilisateurs) sont d'autres arguments de choix.

Les sites de secours (*in situ* ou déportés) se classent selon les types suivants :

- **salle blanche** (une salle machine protégée par des procédures d'accès particulières, généralement secourue électriquement). Par extension, on parle de *salle noire* pour une salle blanche entièrement pilotée à distance, sans aucun opérateur à l'intérieur.
- **site chaud** : site de secours où l'ensemble des serveurs et autres systèmes sont allumés, à jour, interconnectés, paramétrés, alimentés à partir des données sauvegardées et prêt à fonctionner. Le site doit aussi fournir l'ensemble des infrastructures pour accueillir l'ensemble du personnel à tout moment et permet une reprise d'activité dans des délais relativement courts (quelques heures). Un tel site revient quasiment à doubler les capacités informatiques de l'entreprise (on parle de **redondance**) et présente donc un poids budgétaire non négligeable.
- **site froid** : site de secours qui peut avoir une autre utilisation en temps normal (ex : gymnase). Les serveurs et autres systèmes sont stockés mais non installés, connectés, etc. Lors d'un sinistre, un important travail doit être effectué pour mettre en service le site ce qui conduit à des temps de reprise long (quelques jours). Mais son coût de fonctionnement, hors période d'activation, est faible voire nul.
- **site tiède** : site de secours intermédiaire. En général on trouve des machines installées (mise à jour décalée par rapport au site de production) avec les données sur bande mais non importées dans les systèmes de données. [20]

Il est aussi possible d'utiliser des systèmes distribués sur plusieurs sites (diminution du risque de panne par effet de foisonnement) ou un **site de secours mobile** qui correspond à un camion transportant des serveurs et autres systèmes, permettant de n'avoir besoin que d'un système de secours pour plusieurs sites, en tablant sur l'improbabilité qu'une panne touche simultanément plusieurs sites.

Plus les temps de rétablissement garantis sont courts, plus la stratégie est coûteuse. Il faut donc choisir la stratégie qui offre le meilleur équilibre entre le coût et la rapidité de reprise.

D'autre part pour des problématiques de haute disponibilité on a recours aussi à de la redondance mais de manière plus locale.

- Doublement d'alimentation des baies des serveurs,
- Redondance des disques en utilisant la technologie RAID,
- Redondance de serveurs avec des systèmes de *load balancing* (répartition des requêtes) ou de *heartbeat* (un serveur demande régulièrement sur le réseau si son homologue est en fonctionnement et lorsque l'autre serveur ne répond pas, le serveur de secours prend le relais).

Il est aussi possible de recourir à un site secondaire de haute disponibilité qui se situe généralement près du site de production (moins de 10 kilomètres) afin de permettre de les relier avec de la fibre optique et synchroniser les données des deux sites en quasi temps réel de manière synchrone ou asynchrone selon les technologies utilisées, les besoins et contraintes techniques.

✓ **Une bonne information et un bon partage des rôles :**

Quel que soit le degré d'automatisation et de sécurisation d'un système informatique, la composante humaine reste un facteur important. Pour limiter le risque de panne, les acteurs d'un SI (service informatique) doivent adopter les comportements les moins risqués pour le système et éventuellement savoir accomplir des gestes techniques.

- Pour les utilisateurs, il s'agit :
  - de respecter les normes d'utilisation de leurs ordinateurs : n'utiliser que les applications référencées par les mainteneurs du SI, ne pas surcharger les réseaux par des communications inutiles (téléchargements massifs, échanges de données inutiles, rester connecté sans nécessité), respecter la confidentialité des codes d'accès ;
  - de savoir reconnaître les symptômes de panne (distinguer un blocage d'accès d'un délai de réponse anormalement long, par exemple) et savoir en rendre compte le plus vite possible.
- Pour les opérateurs du SI, il s'agit d'avoir la meilleure connaissance du système en termes d'architecture (*cartographie* du SI) et de fonctionnement (en temps réel si possible), de faire régulièrement les sauvegardes et de **s'assurer qu'elles sont utilisables**.
- Pour les responsables, il s'agit de faire les choix entre réalisations internes et prestations externes de manière à couvrir en totalité le champ des actions à conduire en cas de panne (par exemple, rien ne sert d'avoir des machines de secours si on ne prévoit pas la mise à jour de leur système d'exploitation), de passer les contrats avec les prestataires, d'organiser les relations entre les opérateurs du SI et les utilisateurs, de décider et mettre en œuvre les exercices de secours, y compris le retour d'expérience.

▪ **Mesures curatives :**

Selon la gravité du sinistre et la criticité du système en panne, les mesures de rétablissement seront différentes.

- ✓ **La reprise des données :**

Dans cette hypothèse, seules des données ont été perdues. L'utilisation des sauvegardes est nécessaire et la méthode, pour simplifier, consiste à réimplanter le dernier jeu de sauvegardes. Cela peut se faire dans un laps de temps court (quelques heures), si l'on a bien identifié les données à reprendre et si les méthodes et outils de réimplantation sont accessibles et connus.

- ✓ **Le redémarrage des applications :**

A un seuil de panne, plus important, une ou des applications sont indisponibles. L'utilisation d'un site de secours est envisageable, le temps de rendre disponible l'application en cause.

- ✓ **Le redémarrage des machines :**

- provisoire : utilisation des sites de secours
- définitif : après dépannage de la machine d'exploitation habituelle, y rebasculer les utilisateurs, en s'assurant de ne pas perdre de données et si possible de ne pas déconnecter les utilisateurs.

IV.9.2. Développement du plan :

Le plan de reprise contient les informations suivantes :

- La composition et le rôle des « équipes de pilotage du plan de reprise ». Ces équipes se situent au niveau stratégique :

1. les dirigeants qui ont autorité pour engager des dépenses ;
2. le porte-parole responsable des contacts avec les tiers : la presse, les clients et les fournisseurs, etc. ;
3. au niveau tactique, les responsables qui coordonnent les actions ;
4. au niveau opérationnel, les hommes de terrain qui travaillent sur le site sinistré et sur le site de remplacement.

La composition de ces équipes doit être connue et à jour, ainsi que les personnes de remplacement et les moyens de les prévenir. Les membres des équipes doivent recevoir une formation.

- Les procédures qui mettent la stratégie en œuvre. Ceci inclut les procédures d'intervention immédiate (qui prévenir ? qui peut démarrer le plan et sur quels critères ? où les équipes doivent-elles se réunir ? etc.) ;
- Les procédures pour rétablir les services essentiels, y compris le rôle des prestataires externes.

IV.9.3. Exercices et maintenance :

Le plan doit être régulièrement essayé au cours d'exercices. Un exercice peut être une simple revue des procédures, éventuellement un jeu de rôles entre les équipes de pilotage. Un exercice peut aussi être mené en grandeur réelle, mais peut se limiter à la reprise d'une ressource (par exemple, le serveur principal), ou à une seule fonction du plan (par exemple, la procédure d'intervention immédiate). Le but de l'exercice est multiple :

- Vérifier que les procédures permettent d'assurer la continuité d'activité ;
- Vérifier que le plan est complet et réalisable ;
- Maintenir un niveau de compétence suffisant parmi les équipes de pilotage ;
- Évaluer la résistance au stress des équipes de pilotage.

Un plan doit aussi être revu et mis à jour régulièrement (au moins une fois par an) pour tenir compte de l'évolution de la technologie et des objectifs de l'entreprise. La seule façon efficace de mettre à jour le PCA est d'en sous traiter la maintenance aux métiers afin qu'il soit réactualisé à chaque réunion mensuelle de service.

IV.10. Plan de reprise d'activité :

Un **plan de reprise d'activité** (en anglais : *Disaster Recovery Plan* ou *DRP*) permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation.

Le plan de reprise d'activité doit permettre, en cas de sinistre, de basculer sur un système de relève capable de prendre en charge les besoins informatiques nécessaires à la survie de l'entreprise. Il existe plusieurs niveaux de capacité de reprise, et le choix doit dépendre des besoins exprimés par l'entreprise.

On le distingue du *plan de continuité d'activité*, qui permet plutôt de poursuivre l'activité sans interruption du service.

IV.11. Conclusion :

La politique de sécurité permet de transcrire le travail de modélisation effectué pour comprendre les risques et leurs impacts, en des mesures concrètes de sécurité. Sa spécification est un des garants du bon dimensionnement des mesures de sécurité et d'une gestion efficace. Elle donne de la cohérence à la gestion et permet d'adopter vis à vis des risques et menaces, une attitude préventive et pro-active et pas seulement réactive.

Elle permet de lier la stratégie de sécurité de l'entreprise à sa réalisation opérationnelle. Elle doit être dynamique et remise en question de manière permanente afin de suivre l'évolution des systèmes, de l'environnement et des risques.

La bonne réalisation d'une politique de sécurité permet au mieux, de maîtriser les risques informatiques, tout en réduisant leur probabilité d'apparition. Toutefois, il ne faut pas perdre de vue que même un bon gestionnaire de la sécurité, tout en anticipant et prévenant certains accidents volontaires ou non, n'est pas devin. L'on évoque couramment l'intégrité des données, moins souvent celle des hommes. Nul service de sécurité, aussi perfectionné soit-il, ne tient si l'intégrité des administrateurs, responsables réseau, hommes systèmes ou utilisateur se trouve mise en cause. Ne perdons pas de vue que le maillon faible de la sécurité est l'homme.

La sécurité est devenue une activité multidisciplinaire : cryptographie classique, méthodes mathématiques formelles, tatouage électronique, biométrie, ingénierie des réseaux, dispositifs variés de sécurité (carte à puce, pare-feu, système de détection d'intrusion, pots de miel, dispositifs biométriques), infrastructure de sécurité (gestion de certificats pour identifier et authentifier les acteurs dans les transactions du commerce électronique), infrastructure de confiance pour les échanges électroniques (signature électronique de documents contractuels), systèmes de surveillance, méthodologie de validation d'assurance de sécurité, gestion de crises…

Les entreprises et les institutions doivent sans cesse adapter leurs moyens de détection et de lutte informatique : les méthodes traditionnelles et une approche technique ne suffisent plus. La sécurité informatique est désormais assurée par une chaîne complète, organisationnelle et technique.

En outre, la sécurité ne peut être une réalité uniquement si les métiers sont impliqués dans la définition d'une politique : direction générale, direction de production ou direction technique doivent être impliqués dans la démarche, au-delà des DSI et RSSI. L'efficacité opérationnelle des moyens de protection repose pour une large part sur la compréhension des enjeux pour tous les acteurs de l'entreprise, quel que soit leur niveau hiérarchique.

Grâce à un dispositif, à la fois technique et organisationnel. La gamme des méthodes actuelles et des outils existants permet de parer aux erreurs humaines et aux périls qui risquent de porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité des réseaux et des systèmes.
Par ailleurs, la recherche en sécurité est en plein essor. L'objectif est d'améliorer la maîtrise de la circulation des informations sur les réseaux, de favoriser la dissémination des applications informatiques et d'encourager l'appropriation des technologies numériques par un large public.

De nos jours, les systèmes de sécurité informatique sont mis à rude épreuve : stockage de données dans le cloud (informatique en nuage), micropuces omniprésentes, réseaux sociaux… Non seulement la communication permanente sur le réseau expose les systèmes cryptographiques à des légions de connexions menaçantes, mais les mécanismes de sécurité doivent en plus désormais fonctionner sur des appareils à faibles capacités de calcul, comme les téléphones portables notamment les Smartphones de plus en plus utilisés dans le monde professionnel.

On peut dire à la fin que d'un coté les risques augmentent jour après jour mais de l'autre coté la sécurité elle aussi avance en permanence. Entre ces deux cotés, l'acteur essentiel qui peut faire la différence est sans doute le facteur humain qui peut bien renforcer cette sécurité par la mise en place d'une politique efficace à la fois technique et organisationnelle dans un environnement sensibilisé où les différents acteurs sont de plus en plus formés pour adopter les bonnes pratiques en matière de sécurité des systèmes d'information.

[1] : Sécurité informatique (3ème édition) de Laurent Bloch, Christophe Wolfhugel. Édition : Eyrolles - 325 pages, 3eédition, 23 juin 2011

[2] : Tout sur la sécurité informatique de Jean-François Pillou & Jean-Philippe Bay. Édition : Dunod - 262 pages, 3eédition, 1er août 2013

[3] : Solange Ghernaouti-Hélie « Sécurité Informatique et Réseaux » DUNOD 2006.

[4] : Hacker's Guide de Eric Charton. Édition : Pearson Education - 344 pages, 4eédition, 1er septembre 2011

[5] : Hacking Interdit d'Alexandre J. Gomez Urbina. Édition : Micro Application - 1248 pages 2eédition, 1er février 2007

[6] : Les virus informatiques : théorie, pratique et applications d'Eric Filiol. Édition : Springer Verlag - 575 pages, 2eédition, 1er mai 2009

[7] : François Paget, *Vers & Virus - Classification, lutte anti-virale et perspectives*, DUNOD, 2005

[8] : Sécurité informatique - Ethical Hacking (1ère édition) Apprendre l'attaque pour mieux se défendre de Franck Ebel, Sébastien Baudru, Robert Crocfer, David Puche, Jérôme Hennecart, Sébastien Lasson Marion Agé. Édition : ENI - 355 pages, 1re édition, 1er novembre 2009

[9] : Techniques de hacking de Jon Erickson. Édition : Pearson Education - 512 pages, 2eédition, 24 février 2012

[10] : Sécurité informatique de Gildas Avoine, Pascal Junod, Philippe Oechslin Édition : Vuibert - 286 pages, 2eédition, 19 février 2009

[11] : Les bases du hacking de Patrick Engebretson. Édition : Pearson Education - 240 pages , 2eédition, 13 août 2013

[12] : Cryptographie en pratique de Niels Ferguson et Bruce Schneier. Édition : Vuibert - 338 pages, 1er août 2004

[13] : SSL VPN Accès web et extranets sécurisés de Joseph Steinberg, Timothy Speed. Édition : Eyrolles - 206 pages, 1re édition, 1er juillet 2006

[14] : Andrew Hay and Daniel Cid « OSSEC HIDS Host-Based intrusion Detection system », Syngress edition, 2008

[15]: Anne Henmi and Mark Lucas « Firewall policies and VPN Configurations », Syngress edition, 2006

[16] Filtrage Bayésien et Approximation Particulaire version du 29 août 2010 François Le Gland INRIA-Rennes

[17] Vuibert Sciences, Guinier D. - Chapitre : La politique de sécurité, pp. 1486-1498, l'encyclopédie de l'informatique et des systèmes d'information, 2088 pages, Vuibert Sciences, 2006

[18] : Guide des pratiques et retours d'expérience de Bernard Foray. Édition : Dunod - 269 pages, 1re édition, 1er janvier 2007

[19] : Gestion des risques en sécurité de l'information d'Anne Lupfer. Édition : Eyrolles - 230 pages, 1re édition, 1er septembre 2010

[20] : Plan de Continuité d'Activité et Système d'Information : vers l'entreprise résiliente, Matthieu Bennasar, Dunod, 2006 et 2e édition 2010 (prix AFISI 2006, meilleur ouvrage de management des SI).

Les articles de recherche :

[A1] : Evolution de la menace par Philippe Bougeois et Thierry Marronnier (expert en sécurité) 2009. *Réseaux & Télécoms* (*R & T*) magazine d'informatique français, publié par la filiale française du groupe IDG(International Data Group).

Site web http:://www.reseaux-telecoms.com

[A2] : Spam et lutte anti spam par Sébastien Fountaine 2012.

The Hackademy Magazine publication bimestrielle française traitant de hacking en général et de sécurité informatique.

Site web : http:://www.thehackademy.net

[A3] : Les entreprises face aux risques du « cyberespace » par Antoine Cappelle - le 4 février 2014. *Phrack* magazine électronique underground international de langue anglaise édité par et pour des hackers depuis 1985.

Site web : http ://www.phrack.org phrack.org

[A4] : Sécurité : les entreprises tentées par les solutions d'authentification multi-facteurs ? par Perrine Tiberghien, mai 2012. *MISC* (Multi-system & Internet Security Cookbook) Magazine sécurité informatique édité par Diamond Editions.

Site web: http ://www.miscmag.com

[A5] : Pourquoi et comment choisir un VPN pour son entreprise ? (Internet & Réseaux - Conseils business - 11/02/2014) Pierre-François Faure, Responsable Sécurité. *Réseaux & Télécoms* (*R & T*) magazine d'informatique français, publié par la filiale française du groupe IDG (International Data Group).

Site web http ://www.reseaux-telecoms.com

[A6] : RSSI : un métier en pleine évolution, 2012 Jean-Marc Berlioux. SSTIC (Le Symposium sur la sécurité des technologies de l'information et des communications) conférence francophone annuelle sur le thème de la sécurité de l'information.

Site web: http:://www.sstic.org

[A7] : Face à l'évolution technologique et à la multiplicité des problèmes potentiels le directeur sécurité change de dimension par Alain Juillet 2013. SSTIC (Le Symposium sur la sécurité des technologies de l'information et des communications) conférence francophone annuelle sur le thème de la sécurité de l'information.

Site web: http:// www.sstic.org

[A8] : Sécurité informatique : la fin de l'amateurisme dans les PME (Internet & Réseaux) 2013 par Jean-Frédéric Karcher, expert Sécurité. *Réseaux & Télécoms* (*R & T*) magazine d'informatique français, publié par la filiale française du groupe IDG (International Data Group).

Site web http:://www.reseaux-telecoms.com

[A9] : Pensez à manager votre sécurité informatique : Pierre Oger et Laurent Marsal (consultant SSI) 2010. SSTIC (Le Symposium sur la sécurité des technologies de l'information et des communications) conférence francophone annuelle sur le thème de la sécurité de l'information La 11e édition du SSTIC, Rennes du 5 au 7 juin 2013.

Site web: http:// www.sstic.org

[A10] : ISO 17799 ET 27001 nouvelles perspectives normatives par Frédéric Huynh 2005 *Réseaux & Télécoms* (*R & T*) magazine d'informatique français, publié par la filiale française du groupe IDG (International Data Group).

Site web http:://www.reseaux-telecoms.com

Annexe I : Les protocoles de sécurité :

I1. Internet Protocol Security :

IPsec (*Internet Protocol Security*), défini par l'IETF comme un cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques, est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP. IPsec se différencie des standards de sécurité antérieurs en n'étant pas limité à une seule méthode d'authentification ou d'algorithme et c'est la raison pour laquelle il est considéré comme un cadre de *standards ouverts*. De plus, IPsec opère à la couche réseau (couche 3 du modèle OSI) contrairement aux standards antérieurs qui opéraient à la couche application (couche 7 du modèle OSI), ce qui le rend indépendant des applications, et veut dire que les utilisateurs n'ont pas besoin de configurer chaque application aux standards IPsec.

I.2. Remote Authentication Dial-In User Service:

RADIUS (*Remote Authentication Dial-In User Service*) est un protocole client-serveur permettant de centraliser des données d'authentification

I.3. Kerberos :

Est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs. Créé au Massachusetts Institute of Technology, Kerberos a d'abord été mis en œuvre sur des systèmes Unix.

I.4. Password Authentication Protocol (PAP):

Est un protocole d'authentification pour PPP. Les données sont transmises en texte clair sur le réseau ce qui le rend par conséquent non sécurisé.

L'avantage du PAP est qu'il est extrêmement simple à implémenter, lui permettant d'être utilisé dans des systèmes embarqués très légers. Sur des systèmes de taille raisonnable on préférera sans doute le protocole CHAP.

I.5. L'HyperText Transfer Protocol Secure:

plus connu sous l'abréviation **HTTPS** — littéralement « protocole de transfert hypertexte sécurisé » — est la combinaison du HTTP avec une couche de chiffrement comme SSL ou TLS.

HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable (et faisant généralement partie de la liste blanche des navigateurs internet). Il garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans

les formulaires) et reçues du serveur. Il peut permettre de valider l'identité du visiteur, si celui-ci utilise également un certificat d'authentification client.

HTTPS est généralement utilisé pour les transactions financières en ligne : commerce électronique, banque en ligne, courtage en ligne, etc. Il est aussi utilisé pour la consultation de données privées, comme les courriers électroniques, par exemple.

Depuis le début des années 2010, le HTTPS s'est également généralisé sur les réseaux sociaux.

I.6. Protocole AAA :

En sécurité informatique, **AAA** correspond à un protocole qui réalise trois fonctions : l'authentification, l'autorisation, et la traçabilité (en anglais : *Authentication, Authorization, Accounting/Auditing*).

- **Authentification**

Cette première phase consiste à vérifier que l'utilisateur correspond bien à l'identité qui cherche à se connecter. Le plus simple ici consiste à vérifier une association entre un mot de passe et un identifiant, mais des mécanismes plus élaborés peuvent être utilisés tel une carte à puce,…

- **Autorisation**

Cette phase consiste à vérifier que l'utilisateur maintenant authentifié dispose des droits nécessaires, est habilité, pour accéder au système. Elle est parfois confondue avec la précédente sur de petits systèmes, mais sur des systèmes plus importants, un utilisateur peut tout à fait être authentifié (ex : membre de l'entreprise) mais ne pas avoir les privilèges nécessaires pour accéder au système (ex : page réservée aux gestionnaires). L'opération consistant à donner les droits d'accès à l'utilisateur est l'habilitation.

- **Traçabilité**

Pour lutter contre les usurpations de droits, il est souhaitable de suivre les accès aux ressources informatiques sensibles (heure de connexion, suivi des actions, …).

Liste de protocoles AAA :

- RADIUS
- Diameter
- TACACS
- TACACS+

- D'autres protocoles utilisés généralement avec les protocoles AAA :

- PPP
- EAP
- LDAP

I.7. Transport Layer Security (TLS), et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet

TLS fonctionne suivant un mode client-serveur. Il fournit les objectifs de sécurité suivants :

- l'authentification du serveur.
- la confidentialité des données échangées (ou session chiffrée).
- l'intégrité des données échangées.
- de manière optionnelle, l'authentification ou l'authentification forte du client avec l'utilisation d'un certificat numérique.
- la spontanéité, c'est-à-dire qu'un client peut se connecter de façon transparente à un serveur auquel il se connecte pour la première fois.
- la transparence, qui a contribué certainement à sa popularité : les protocoles de la couche d'application n'ont pas à être modifiés pour utiliser une connexion sécurisée par TLS. Par exemple, le protocole HTTP est identique, que l'on se connecte à un schème http ou https.

I.8. WS-Security (Web Services Security):

Est un protocole de communications qui permet d'appliquer de la sécurité aux services web. Le protocole contient des spécifications sur la façon dont l'intégrité et la confidentialité peuvent être appliquées aux messages de services web

Annexe II : Le marché de la sécurité informatique

II.1.Les entreprises face au défi de la sécurité informatique :

La fréquence des cyber-attaques aurait doublé l'an dernier, selon l'entreprise de sécurité informatique américaine FireEye: leur rythme serait passé de une toutes les trois secondes en 2012 à une toutes les 1,5 seconde en 2013.

73 % des directions informatiques mondiales interrogées par le cabinet britannique Vanson Bourne pour Dell affirment ainsi avoir déjà été l'objet d'une faille de sécurité depuis un an. 17 % en moyenne du budget d'une direction informatique est dédié à la sécurité et 74 % d'entre elles prévoient d'augmenter celles-ci au cours des deux ou trois années à venir.

- **Les PME sont les plus vulnérables :**

Paradoxe: les entreprises les moins prêtes à investir pour se protéger sont les PME, précisément les plus vulnérables. Car les cyberpirates savent que la plupart d'entre elles sont la clé d'entrée vers les grandes sociétés dont elles sont les sous-traitants. Le marché reste donc porteur.

II.2. Marché de la sécurité informatique :

Le marché mondial des applications de sécurité a connu une croissance de l'ordre de 7,9% selon la société d'études Gartner. Les dépenses dans les logiciels de sécurité sont influencées par l'évolution des nouvelles menaces informatiques.

D'après Gartner, la montée du nombre d'attaques informatiques, en particulier les menaces affectant les périphériques dans le cadre des politiques BYOD (Bring your own device) a poussé les entreprises à se sécuriser de plus en plus. En conséquence, le nombre de logiciels de sécurité vendus a connu une croissance de l'ordre de 7.9% par rapport à l'année 2011. En effet, selon les estimations de Gartner, les concepteurs de solutions de sécurité ont généré 19,2 milliards de dollars de rente en 2012.

Par ailleurs, selon l'étude, malgré le fait que le marché mondial de solutions de sécurité a continué à croître, le niveau de croissance n'est pas le même, la situation varie d'une région à une autre. En Eurasie, la région a connu une croissance à deux chiffres, encouragée par une économie dynamique et de nouveau projets technologiques. Mais ce n'est pas le cas en Europe de l'Ouest qui reste à la traîne, à cause de la fragilité de l'économie.

II.2.1. Classement des éditeurs de logiciels de sécurité :

Table 1. Top Security Software Vendors, Worldwide, 2011-2012 (Millions of Dollars)

Company	2012 Revenue	2012 Market Share (%)	2011 Revenue
Symantec	3,747.1	19.6	3,652.0
McAfee*	1,680.0	8.8	1,226.0
Trend Micro	1,172.0	6.1	1,205.1
IBM	953.6	5.0	931.3
EMC	717.6	3.7	716.1
Others	10,865.2	56.8	10,008.7
Total	**19,135.5**	**100.0**	**17,739.2**

Symatec conserve sa position de leader dans le secteur de sécurité informatique. Avec une part de marché à 19,6%, il a généré 3.7 milliards de dollars de revenus. Vient par la suite, **McAfee** qui a réalisé un chiffre d'affaires de l'ordre de 1,68 milliard de dollars, avec 37%. Cette situation s'explique par l'acquisition de la société McAfee par **Intel**.

La troisième place est occupée par **Trend Micro** qui a vu ses ventes de sécurité chuter de 2,7%, avec un chiffre d'affaires de l'ordre de 1,17 milliard de dollars. Suivi par deux entreprises américaines **IBM** et **EMC** avec respectivement 953,6 et 717,6 millions de dollars.

Enfin, les autres fournisseurs d'applications de sécurité ont réalisé 10,86 milliards de dollars.

II.2.2. Dépenses gouvernementales :

Voici à titre de comparaison les budgets de quelques agences gouvernementales qui s'intéressent à la cybersécurité :

- Cyber Command américain pour l'année 2013 : 182 millions de dollars américains.
- Agence nationale de la sécurité des systèmes d'information française : 90 millions d'euros pour l'année 2012.
- Bundesamt für Sicherheit in der Informationstechnik allemand : 70 millions d'euros en 2011.