Paris Graduate School of Management
ECOLE SUPERIEURE DE GENIE INFORMATIQUE

ECOLE SUPERIEURE DE GESTION D'INFORMATIQUE ET DES SCIENCES

INGENIERIE INFORMATIQUE RESEAUX ET SECURITE

MEMOIRE DE RECHERCHE

Année 2008

LES STRATEGIES DE SECURITE ET SYSTEMES DE PROTECTION CONTRE LES INTRUSIONS

Présenté par
MESSAVUSSU Adotevi Enyonam
MOUMOUNI MOUSSA Harouna

Sous la direction de
M. ATOHOUN Béthel
Chef département IIR ESGIS

Décembre 2008

Remerciements

Nos très sincères remerciements vont à :

- M. Thierry MONLOUIS : Le Directeur de l'ESGI de Paris et tout son personnel ;
- M. Macy AKAKPO : Le Directeur Général du Groupe ESGIS ;
- M. Pascal DANON : Le Conseiller pédagogique du Groupe ESGIS ;
- M. Béthel ATOHOUN : Le Conseiller chargé de l'Informatique, du réseau et du Cycle Ingénieur IIR du Groupe ESGIS ;
- A l'ensemble du personnel du Groupe ESGIS à Lomé et à Cotonou ;
- M. Alain AINA : Le Directeur Technique par intérim d'AfriNIC et Directeur de TRS.
- Mme Martine OUENDO pour sa bienveillance et sa chaleureuse hospitalité ;

Pour MOUMOUNI MOUSSA Harouna

- A mes très chers parents MOUMOUNI MOUSSA et Hassana MAMOUDOU, je vous dédie ce travail qui n'est rien d'autre qu'un fruit de votre indéfectible soutien ;
- A mon oncle Issou MAMOUDOU et sa famille, pour le soutien inconditionnel apporté durant ce parcours ;
- A mon frère Abdoul et mes sœurs Mariama, Hawa, Adama et Nadia, en espérant vous servir de modèle ;
- A mes amis de longue date pour leurs encouragements qui ne m'ont jamais fait défaut : Seyni, Douma, Chaibou, Yann, Salélé, …
- A ma nièce Zeinab en espérant te donner déjà le goût du travail, surtout bine fait ;
- Au personnel de BENIN TELECOMS ; en particulier à Joseph HONVO, Louis AGBAHOLOU et Maxime GODONOU-DOSSOU pour leurs constantes disponibilités ;
- A Nsilu MOANDA Vodacom RDC pour ses multiples conseils et son assistance qui ne m'ont jamais fait défaut durant ce parcours ;
- A tous mes proches que je n'ai pu citer ici.

Pour MESSAVUSSU Adotevi Enyonam

- A mes feux très chers parents MESSAVUSSU Adovi Koffi et MIKEM Adévi Martine à qui je dédie ce mémoire ;
- A mon cousin et grand frère Franck TIGOUE, sa femme Claudine, ses frères et ses enfants Chris et William pour leur soutien indéfectible et leur confiance sans faille en mes capacités ;
- A mes tantes Mme MESSAVUSSU Anyélégan Essivi et Mme TIGOUE Benedicta née MESSAVUSSU, mon oncle Prosper MESSAVUSSU pour m'avoir supporté et soutenu tout au long de ce cycle ingénieur ;
- A mes frères M. MESSAVUSSU Adoté Kossi (John), Ernesto, Moïse et à ma sœur Bélinda pour leurs encouragements;
- A mon fils Claude Junior MESSAVUSSU et à sa mère HOUTONDJI Akouavi Djéné pour leur amour qui m'a toujours inspiré ;
- A mes sœurs AGBODAZE Amévi Tékla, ATAYI Ayikoélé Augustine, mon frère AGBODAZE Kodjo Gloria et mes tantes MIKEM Mamavi et TEOURI Ryssala ;
- A tous mes amis sincères Muriel, Roland, Kézié, Claire, Jérémie, Hervé et Benny.
- Et à tous mes proches, amis et connaissances que je n'ai pas pu citer ici

Résumé

En se basant sur les études et enquêtes menées à travers le monde, on se rend bien compte qu'il devient de plus en plus compliqué de garantir la sécurité des systèmes d'informations. Cette situation qui est essentiellement due à la multiplication inquiétante des menaces en matière de sécurité informatique s'explique par la prolifération des outils permettant de réaliser les attaques informatiques et par la décroissance continue du niveau de connaissance nécessaire pour l'utilisation de ces outils. Face à cette situation, de nouvelles solutions et mesures de sécurité n'ont pas aussi cessé de voir le jour et de se proliférer.
Cependant le problème qui se pose toujours c'est de savoir comment mettre en place ces mesures et solutions de sécurité efficacement afin de réellement protéger les systèmes d'information car le fait de juxtaposer et de multiplier les solutions de sécurité sans analyser au préalable leur compatibilité et leurs objectifs respectifs n'a jamais été une solution fiable. Dans ce contexte, les stratégies de sécurité dont l'implémentation se traduit par la définition et la mise en application d'une politique de sécurité constituent le meilleur moyen d'atteindre les objectifs de la sécurité informatique.
Malheureusement, on se rend bien compte aujourd'hui que malgré toutes les mesures et stratégies de sécurité qu'on peut mettre en place, les systèmes d'informations restent néanmoins vulnérables à certaines attaques ciblées ou à des intrusions. C'est pourquoi depuis quelques années, les experts de la sécurité parlent de plus en plus d'un nouveau concept à savoir la détection d'intrusion. L'étude de la détection d'intrusion nous permettra de mieux comprendre les systèmes de détection et de prévention d'intrusions et de voir comment ils arrivent à renforcer la sécurité en fermant les trous de sécurité laissés par les mesures classiques de sécurité.

Abstract

While basing oneself on the studies and surveys carried out throughout the world, one realizes well that it becomes increasingly complicated to guarantee the information system security. This situation which is primarily due to the worrying multiplication of the threats as regards computer security can be explained by proliferation of the tools making it possible to carry out cyber attacks and by the decreasing level of knowledge necessary for the use of these tools. Vis-a-vis this situation, new solutions and safety measures are invented.
However the difficulty which always arises it is to find the way how to set up these measurements and solutions of safety effectively in order to really protect the information systems because the fact of juxtaposing and multiplying the solutions of safety without first analyzing their respective compatibility and their objectives was never a reliable solution. In this context, the strategies of safety whose implementation results in the definition and the implementation of a policy of safety constitute the best means of achieving the goals of the computer security.
Unfortunately, one realizes well today that despite every measurements and strategies of safety which one can set up, the information systems remain nevertheless vulnerable to certain targeted attacks or intrusions. This is why for a few years; the experts of safety have spoken more and more about a new concept which is intrusion detection. The study of intrusion detection will enable us to better understand the intrusion detection and prevention systems and to see how they can be managed to reinforce safety by closing the safety holes left by traditional safety measurements and solutions.

Table des matières

Table des illustrations

Liste des tableaux

Introduction

La valeur de notre civilisation se déplace inéluctablement vers la sphère immatérielle. La miniaturisation continue de l'électronique, l'accélération des performances des réseaux de communication et le déploiement inexorable des infrastructures informatiques édifient une urbanisation digitale qui favorise l'accès à l'information et facilite la communication. Cette évolution de l'informatique, de l'électronique, et surtout des systèmes distribués a malheureusement contribué à faire évoluer de manière considérable les menaces informatiques. Les risques auxquels sont confrontées les entreprises et les organisations aujourd'hui sont tels que la sécurité informatique prend une place de plus en plus prépondérante et vitale au sein des institutions privées et publiques. Il ne s'agit plus de considérer la sécurité comme un luxe réservé aux grandes organisations ou entreprises car il n'est pas rare d'assister de nos jours à des prises d'otages de petits systèmes ou réseaux afin de s'en servir comme relais pour réaliser des attaques de grandes envergures sur de gros systèmes ou réseaux.

Au même moment, le niveau de connaissance requis pour devenir pirate ne cesse de diminuer en raison de la prolifération d'outils et de logiciels malfaisants (*malwares*) disponibles gratuitement sur le web. Vue cette situation inquiétante, pour survivre et poursuivre, avec un minimum de sécurité leurs activités, les entreprises et les organisations doivent adopter et mettre en œuvre des stratégies de sécurité. Ces dernières sont en fait des ensembles cohérents et compatibles de mesures de sécurité qui visent à protéger les systèmes d'informations des entreprises des attaques et d'incidents de toutes sortes, ou d'en réduire autant que possible les impacts.

Toutefois, il arrive parfois que des incidents de types intrusions ou attaques surviennent malgré toutes les mesures et stratégies de sécurité mises en place. Ces incidents qui sont de plus en plus nombreux peuvent provenir de l'intérieur comme de l'extérieur des réseaux des entreprises ou des organisations. Face à cette situation, de nouveaux systèmes de surveillance (les systèmes de détection d'intrusion ou IDS) et de protection (les systèmes de prévention d'intrusion ou IPS) sont développés depuis quelques années par les éditeurs de solutions de sécurité. Malheureusement, ces outils sont encore méconnus et très rarement utilisés en Afrique.

Dans la première partie de ce document, nous avons réalisé une étude concernant l'évolution des menaces et solutions en matière de sécurité informatique qui a débouchée sur un état des lieux de la sécurité informatique dans le monde. Dans la deuxième partie, nous avons mis en évidence la nécessité pour les organisations d'aller vers une vision plus large de la sécurité de leurs systèmes d'informations à travers les stratégies et politiques de sécurité. C'est dans ce sens que nous avons concrétisé cette approche par l'application de la méthode MEHARI à une PME du Bénin. La troisième et dernière partie de ce document a pour objectif de montrer l'intérêt pour nos entreprises (ouest africaines dans une moindre mesure et africaines en général) d'une mise en place efficace et stratégique de nouveaux systèmes de surveillance et de protection contre les intrusions afin de renforcer la sécurité au sein des infrastructures informatiques et réseaux.

Chapitre 1 : Evolutions de la sécurité informatique

I.1 Evolutions de l'informatique

L'informatique peut-être définie de manière classique comme la science du traitement automatique et rationnelle de l'information. Son outil par excellence est l'ordinateur. L'informatique a connu des évolutions et parfois des révolutions qui se sont succédé au cours des années.

L'ère des ordinateurs modernes a commencé avec le développement de l'électronique au cours de la Seconde Guerre mondiale, ouvrant ainsi la porte à la réalisation concrète de machines opérationnelles. Au même moment, le mathématicien Alan Turing théorisait le premier sur la notion d'ordinateur, avec son concept de machine universelle. L'informatique est donc une science des temps modernes, même s'il trouve ses origines dans l'antiquité (avec la cryptographie) ou dans la machine à calculer de Blaise Pascal, au XVIIe siècle. Ce n'est qu'à la fin de la Seconde Guerre mondiale qu'elle a été reconnue comme une discipline à part entière et a développé des techniques et des méthodes qui lui étaient propres.

Dans les années 40, un ordinateur occupait une place gigantesque et était très fréquemment soumis à des pannes. En 1947, l'invention des semi-conducteurs a permis de réaliser des ordinateurs plus petits et d'une plus grande fiabilité. Dans les années 50, les grandes organisations commencèrent à utiliser de gros ordinateurs de gestion fonctionnant avec des programmes sur cartes perforées. Puis à la fin des années 50, les circuits intégrés qui combinaient quelques transistors sur une petite puce firent leur apparition. Les années 60 virent l'utilisation massive des systèmes d'ordinateurs centraux desservant des terminaux.

Au début des années 70, le premier microprocesseur, l'Intel 4004 faisait son apparition. Il permettait d'effectuer des opérations sur 4 bits simultanément. En 1981, IBM commercialise le premier « PC » composé d'un processeur 8088 cadencé à 4.77 MHz.

Actuellement, il est très difficile de suivre l'évolution des microprocesseurs. En effet, cette évolution suit la loi de Moore qui fut énoncée en 1965 par Gordon Moore, cofondateur d'Intel qui veut que le nombre de transistors sur un processeur double tous les deux ans, augmentant ainsi ses performances. Intel est déjà arrivé à mettre jusqu'à 1,7 milliard de transistors sur une puce de 65 nm (Montecito). Pour comparaison, le fameux Pentium 4 (3,4 GHz) qu'on a tant décrié était en fait une puce de 90 nm avec seulement 125 millions de transistors. Aujourd'hui, Intel réussi à réduire la taille des puces à 45 nm.

La miniaturisation des composants et la réduction des coûts de production, associées à un besoin de plus en plus pressant de traitement des informations de toutes sortes (militaires, scientifiques, financières, commerciales, etc.) ont entraîné une diffusion de l'informatique dans tous les secteurs d'activités humaines. Quant à l'Afrique, ce n'est que dans les années 1980 qu'elle a vu le début du développement de l'informatique.

La notion de réseau informatique connaît aussi depuis près de quatre décennies, d'énormes transformations et évolutions. C'est au début des années 60 que furent constitués les premiers réseaux avec l'apparition des modems. Ces derniers servaient à connecter des terminaux passifs à un ordinateur central. Les modems avaient une vitesse de 300 bits/s, soit une trentaine de caractères par seconde. Ensuite, dans les années 70, les systèmes BBS (Bulletin Board System) apparaissaient. Ils offraient des services informatisés d'échanges d'informations, auxquels les utilisateurs pouvaient se connecter notamment pour afficher des messages et y répondre. La vitesse de connexion était encore de 300 bits/s. Dans les années 80 les systèmes BBS sont devenus très répandus et la vitesse de 300b/s est très vite devenue

insuffisante pour le transfert des documents volumineux comme les graphiques. Dans les années 1990, le débit des modems est passé à 9600 bits/s. En 1998, la vitesse standard de 56 Kbits/s, a été atteinte.

Les médias de transmission sont passés des câbles coaxiaux aux paires torsadées pour enfin aboutir à la fibre optique qui est actuellement très prisée quand il s'agit de réaliser les réseaux fédérateurs (*backbones*).

Il existe aussi des réseaux sans fil dont l'intérêt le plus évident est la mobilité (c'est-à-dire la liberté de mouvement des utilisateurs). Ces réseaux ont connu depuis leur apparition, des évolutions majeures. La première norme pour ces réseaux est le IEEE 802.11. Elle a été publiée en 1997. Elle offrait un débit de 1 ou 2 Mbits/s à une fréquence de 2,4 GHz. La deuxième (IEEE 802.11a ; jusqu'à 54Mbits/s à 5 GHz) et la troisième norme (IEEE 802.11b ; 11 Mbits/s et 2,4 GHz pour la fréquence) apparurent autour de 1999. D'autres normes dans ce domaine continuent d'être réalisées.

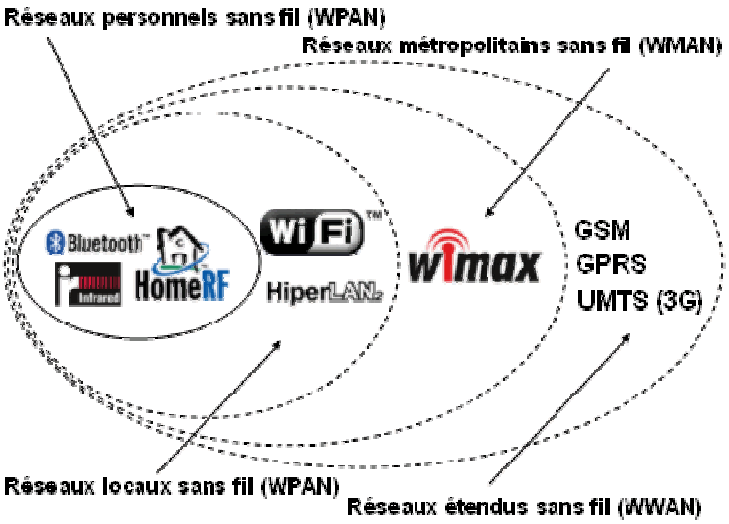


Figure 1-1 : Catégories de réseaux sans fils

Parmi les réseaux sans fils on retrouve le Bluetooth, le wifi, le Wimax et les réseaux sans fil des télécommunications (GSM, GPRS, UMTS etc.).

Ainsi, tout a débuté avec le concept de l'informatique centralisée avec de très grands ordinateurs qui occupaient de grandes salles avec plusieurs terminaux qui gravitaient tout autour. Ensuite on est passé à l'informatique à distance avec l'utilisation des modems en empruntant les réseaux publics de télécommunication. Et déjà à cette étape se posait le problème des lignes téléphoniques qui n'étaient pas gérées par les entreprises elles mêmes. Comment pouvait-on garantir la sécurité des informations qui y transitaient ? L'autre souci majeur que créait l'Informatique centralisée que ce soit à distance ou non c'était que toutes les applications résidaient sur une seule et même machine. Ce qui faisait qu'en cas de panne ou d'accident, une entreprise pouvait tout perdre en un bref instant.

Après cette étape, est arrivée celle de l'informatique distribuée que nous connaissons maintenant avec l'introduction par exemple de multiples serveurs chacun dédié à une tâche bien spécifique. Dans les systèmes distribués, on peut retrouver par exemple pour une institution bancaire un serveur pour la paie, un autre pour gérer la reconnaissance des signatures des clients, un autre pour gérer les comptes des clients etc. Le défi réel était donc de trouver un moyen de faire fonctionner tout cet arsenal de serveurs ensemble. Il s'agissait surtout d'éviter aux utilisateurs d'avoir à s'authentifier (login) sur chaque serveur. Des

systèmes centralisés d'authentification ont donc vu le jour. Il s'agit des systèmes comme Kerberos, Radius, Samba, Active Directory etc.

Avec le développent des réseaux, un nouveau type réseau a vu le jour. Il s'agit d'Internet. Aujourd'hui, avec Internet, on assiste à une unification des réseaux. Ainsi, les intérêts de la mise en place d'un réseau sont multiples, que ce soit pour une entreprise ou un particulier.

Après avoir décortiqué les différentes étapes de l'évolution de l'informatique et des réseaux, nous allons passer en revue les menaces en matière de sécurité informatique.

I.2 Les menaces en matière de sécurité informatique

Le concept de la sécurité informatique et de l'Internet n'a cessé de changer de visage et de dimension au même titre que l'évolution des technologies ; au cours des années 1940, la notion de sécurité informatique était essentiellement axée sur des aspects physiques. Il suffisait de sécuriser l'accès physique à l'ordinateur central (Mainframe), aux terminaux et aux médias de connexion pour empêcher tout accès aux individus non autorisés. Il était d'autant plus facile de garantir la sécurité des données puisqu'on pouvait déterminer à l'avance toutes les portes d'accès possibles et développer sa stratégie de sécurité.

La sécurité des réseaux a toujours été une préoccupation. Il a toujours existé des entités décidées à mener des actions peu recommandables à l'égard des systèmes.

Le nombre d'incidents de sécurité rapportés au *Computer Emergency Response Team Coordination Center* (CERT) augmente chaque année de façon exponentielle. Moins de 200 en 1989, environ 400 en 1991, 1400 en 1993 et 2241 en 1994. Au cours de la décennie 1988-1998 le nombre d'incidents rapportés atteignit les 16.096. Ils se produisent sur les sites gouvernementaux et militaires, parmi les grosses compagnies, dans les universités et dans les petites entreprises. Certains incidents n'impliquent qu'un seul compte sur un système, tandis que d'autres peuvent impliquer plus de 500 000 systèmes à la fois. Ces nombres ne sont bien sûr que la partie émergée de l'iceberg. De nombreuses intrusions ou violations de sécurité ne sont souvent pas déclarées au Centre de Coordination du CERT ou aux autres organisations de réponse aux incidents de sécurité. Dans certains cas c'est parce que les organisations victimes préfèrent éviter toute publicité ou accusation d'imprudence, dans d'autres cas c'est parce que les intrusions ne sont même pas détectées. On ne peut estimer le nombre d'intrusions réellement détectées par les sites attaqués, mais la plus grande partie de la communauté des experts en sécurité informatique pense qu'il ne s'agit que d'un faible pourcentage. Bill Chestwick, des AT&T Bell Labs, pense que sur les attaques réussies, au moins 40% des attaquants accèdent à un compte super-utilisateur (*source Firewalls Digest, 31 mars 1995*).

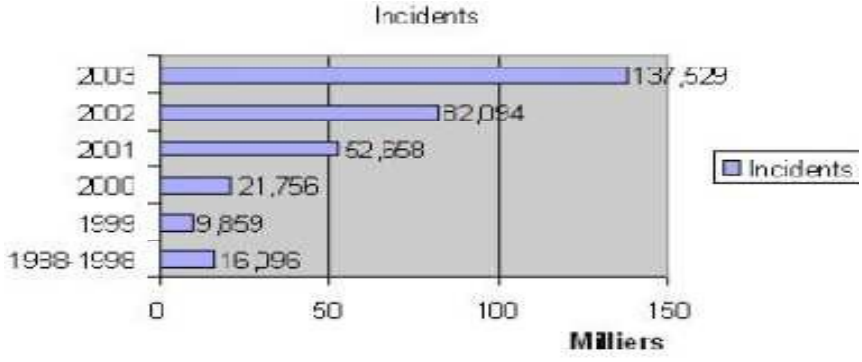


Figure 1-2 : Statistiques des incidents informatiques dans le monde de 1988 à 2003

Le cyberespace est un monde dangereux, et trop peu s'en rendent compte. Aux premiers jours de l'Internet, les sites connectés au réseau disposaient en général d'équipes entières de gourous s'occupant du matériel et du logiciel. Aujourd'hui, se connecter à Internet est devenu si banale que les utilisateurs oublient qu'il faut une certaine sophistication technique pour se connecter en toute sécurité.

Les progrès technologiques ne profitent malheureusement pas qu'aux utilisateurs légaux ; ils sont aussi mis à contribution pour améliorer les techniques de violation des politiques de sécurité. Les techniques d'attaques ont connu une évolution remarquable au cours de ces vingt (20) dernières années, les outils permettant d'attaquer les systèmes d'informations sont devenus bien plus puissants et plus facile à utiliser. Cette facilité d'utilisation a abaissé le niveau de connaissances techniques nécessaires pour lancer une attaque, augmentant en conséquence de façon exponentielle le nombre d'assaillants potentiels.

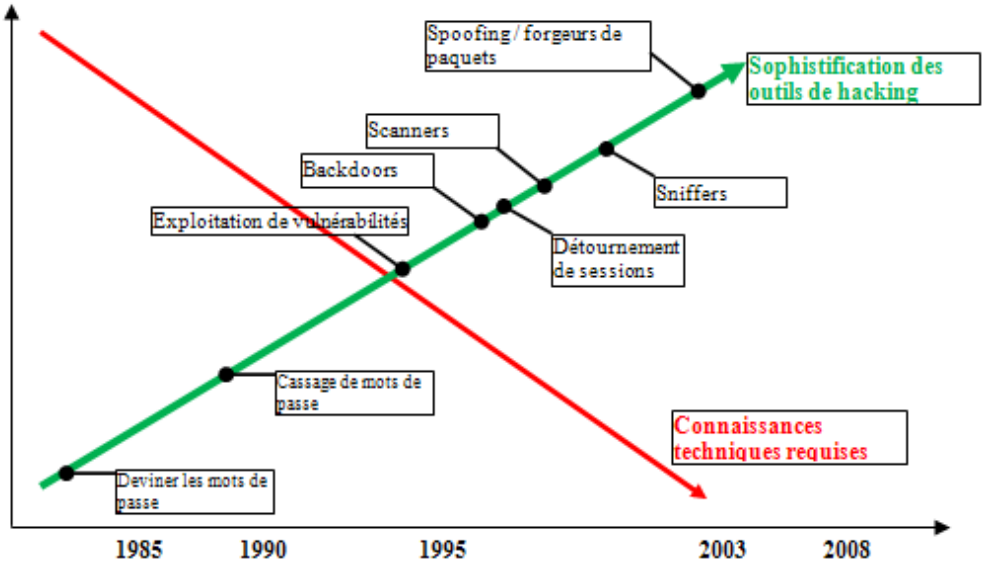


Figure 1-3 : Rapport entre sophistication des outils et niveau de connaissance requis

Dans cette partie de notre document, nous allons tenter de catégoriser les dangers ou les risques auxquels sont exposés les systèmes d'information en deux grandes catégories que nous décortiquerons successivement en profondeur. Il s'agira de voir dans un premier temps les dangers que l'on appelle parfois aussi risques ou attaques informatiques en général et dans un deuxième temps nous parlerons du cas spécial des intrusions.

I.2.1 Les attaques informatiques

Une attaque informatique est l'exploitation d'une faille d'un système (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur Internet des attaques ont lieu en permanence. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (appelées botnets) par des virus, des chevaux de Troie, des vers et autres, à l'insu de leur propriétaire. 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 ;

- glaner des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- 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.

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. 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 :

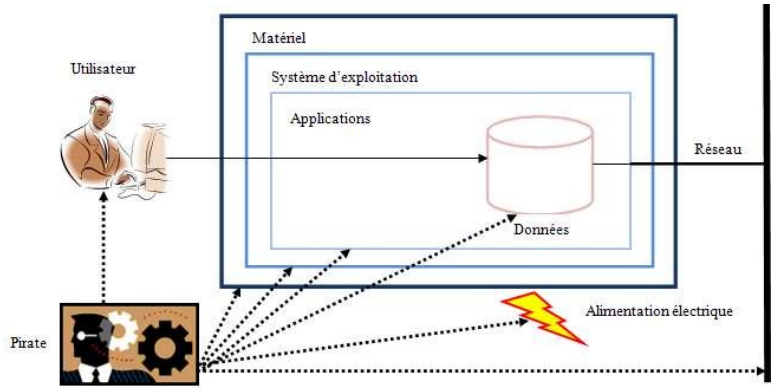


Figure 1-4 : Les niveaux de vulnérabilité d'un système informatique

Il y a d'abord les attaques qui visent l'accès physique et l'environnement du système d'information. Il s'agit des cas où l'attaquant a accès aux locaux et éventuellement même aux machines. Il s'agit souvent des événements comme :

- Les coupures de l'électricité ;
- L'extinction manuelle des ordinateurs ou des serveurs ;
- Le vandalisme ;
- L'ouverture des boîtiers des ordinateurs et le vol des disques durs ou d'autres composants ;
- L'écoute directe du trafic sur le réseau c'est-à-dire en se branchant directement sur le backbone ou sur un core-switch (commutateur principal) par exemple.

Ces attaques que l'on pourrait qualifier de basiques étaient surtout à la mode quand l'informatique était encore à ses débuts. C'est-à-dire l'ère de l'informatique centralisée.

Après les attaques visant les accès physiques et l'environnement, il y a celles utilisant les interceptions des communications comme :

- L'usurpation de ressources ou des paramètres d'identité (mots de passe, adresses IP, adresses MAC) ;
- Le détournement ou altération de messages (Man In the Middle, Brute Force attack etc.);
- Le vol de session (session hijacking), l'ARP poisoning, l'écoute réseau, le balayage de ports etc.

Ensuite, il y a les attaques de type déni de service. Il s'agit des attaques visant à perturber le bon fonctionnement d'un service du système d'exploitation ou d'une application. On distingue habituellement les types de déni de service suivant :

- Exploitation de faiblesses des protocoles TCP/IP ;
- Exploitation de vulnérabilité des logiciels serveurs.

Parmi les techniques utilisées pour réaliser ce type d'attaque, on peut citer les attaques par réflexion, les attaques « Ping de la mort » (ping of death), les attaques par fragmentation, les attaques Land, les attaques SYN etc.

Pour terminer la première partie de cette typologie des attaques informatiques, nous allons citer les arnaques réalisées grâce aux outils informatiques. Il y a dans cette sous catégories l'ingénierie sociale, le scam, le phishing (qui prend de l'ampleur ces dernières années) et enfin les fausses loteries d'Internet (Hoax en anglais).

L'ingénierie sociale a atteint quant à elle un nouveau degré de sophistication, avec notamment le cheval de Troie « Small.DAM » qui a causé des ravages considérables en janvier 2007. Sous couvert des gros titres de l'actualité liés à de véritables événements tels que les tempêtes qui se sont produites en Europe en janvier, il a réussi à se propager dans le monde entier en une seule nuit.

La Turquie, qui en mai de cette année 2008 avait crée la surprise en dépassant les Etats-Unis, demeure un des premiers pays en matière de phishing. Elle talonne en effet les Etats-Unis à 20,10%. En mai 2008, cette part était de 24,36%, contre 16,94% pour les Etats-Unis. La Pologne, déjà classée depuis plusieurs mois avec près de 10% des attaques de phishing, fait un nouveau bond pour atteindre les 15%. La Chine, si elle héberge de nombreux sites infectés, reste sous le seuil des 7%, après toutefois être montée jusqu'à 9% en mai.

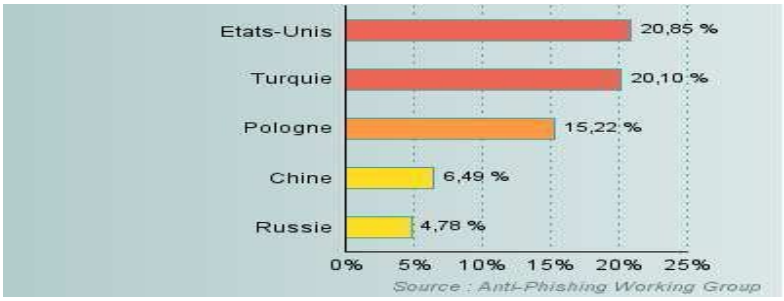


Figure 1-5 : Répartition des attaques de phishing

Souvent, lors des attaques, les pirates gardent toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle ils privilégient habituellement les attaques par rebond (par opposition aux attaques directes), consistant à attaquer une machine par l'intermédiaire d'une autre, afin de masquer les traces permettant de remonter à lui (telle que son adresse IP) et dans le but d'utiliser les ressources de la machine servant de rebond. Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel car il est possible de se retrouver « complice » d'une attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.

Avec le développement des réseaux sans fils, les attaques sont encore plus faciles à réaliser surtout lorsque le réseau sans fil est mal sécurisé, un pirate situé à proximité peut l'utiliser pour lancer des attaques.

Toutes attaques confondues, la Chine qui rassemblait à elle seule 42,96% des menaces en mai de cette année 2008, ne représente plus que 12,95% de celles-ci. Les Etats-Unis ont récupéré

la première place à 25,91%, devant deux pays forts en matière de phishing, à savoir la Turquie et la Pologne. La Russie souvent présentée comme un état source d'attaques double sa part entre mai et juin, pour s'établir à 5,54%.

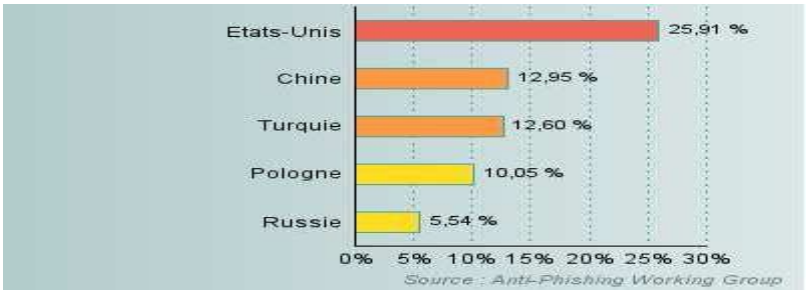


Figure 1-6 : Répartition globale des attaques (toutes catégories confondues)

En matière de courriers indésirables (spam), le nombre de campagnes des deux superpuissances du spam que sont les Etats-Unis et la Chine était de nouveau à la hausse en Juin 2008 par rapport à mai 2008. Une augmentation était également à noter pour la Russie.

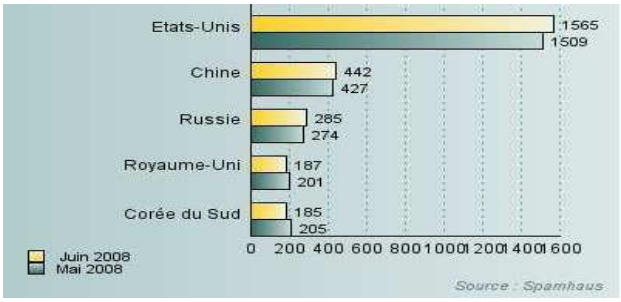


Figure 1-7 : Campagnes de spam par pays en Mai et Juin 2008

En revanche, les campagnes d'origines britannique et coréenne étaient elles en recul d'un mois sur l'autre. Ces pays enregistraient pourtant une hausse en mai. Les autres nations émettrices de spam étaient, par ordre décroissant : Allemagne (178), Japon (153), France (145), Brésil (128) et l'Inde (127).

Il y a aussi des vulnérabilités du web qui sont souvent exploitées pour réaliser des attaques. Parmi elles, on a la manipulation d'URL, le « Cross-Site Scripting » et les injections SQL.

En ce qui concerne les pays hébergeurs de sites malveillants, le graphe suivant nous éclaire suffisamment. D'après le dernier rapport de l'association StopBadware.org (Juin 2008), les sites Web malveillants se concentrent en Chine. Ainsi sur 200 000 sites infectés, 52% sont hébergés sur des réseaux chinois.

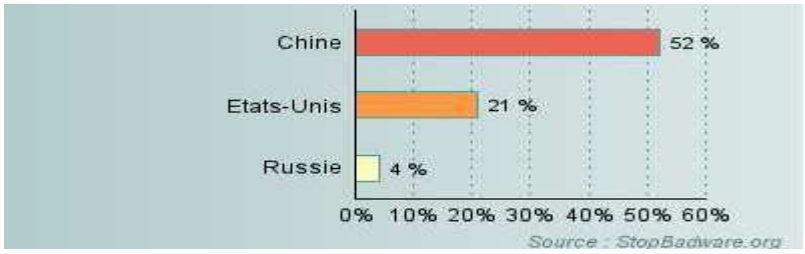


Figure 1-8 : Pays hébergeurs de sites malveillants

Les Etats-Unis arrivent loin derrière avec 21% de sites dangereux. Quant aux autres pays, ils ne dépassent pas le seuil des 4%. Cette position de la Chine est l'une des grandes tendances notée par StopBadware par rapport à 2007. Le premier réseau hébergeur de sites malveillants

était alors américain (iPower) avec 10 000 sites. Il s'agit désormais de CHINANET-BACKBONE avec 50 000.

Aujourd'hui, les menaces informatiques servent même des objectifs et des intérêts politiques. C'est dans ce sens que récemment dans le conflit qui a opposé la Russie et la Géorgie, les sites Web du gouvernement géorgien ont été victimes d'attaques en déni de service visiblement relayées par des hébergeurs russes selon les accusations de la Géorgie

Avec une menace qui s'est déplacée progressivement de la messagerie vers les sites Web, et qui cible donc désormais les navigateurs, les habitudes et les pratiques des internautes à l'égard de ces derniers sont devenues capitales. Confrontés de plus en plus à des pages Web malveillantes, exploitant par exemple une faille dans le navigateur, les internautes sont en effet plus exposés désormais. La sécurité, ou du moins la robustesse du navigateur est devenue donc un critère majeur. Selon le magazine *JDN Solutions*, des chercheurs en sécurité ont révélés que seuls 60% des internautes utilisent un navigateur à jour et que 40% utilisent un navigateur à risque. Les utilisateurs de Firefox seraient les plus rigoureux. Ceux d'Internet Explorer seraient en revanche plus laxistes.

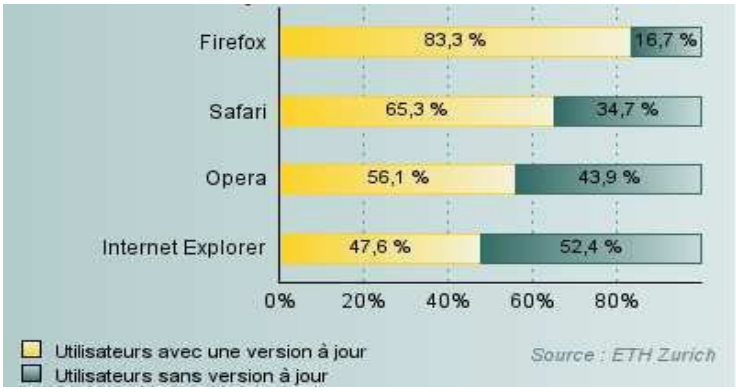


Figure 1-9 : Part des versions des navigateurs les plus sécurisés

Ainsi, ce sont respectivement 83,3% des utilisateurs de Firefox, 65,3% de Safari, 56,1% d'Opera et 47,6% d'Internet Explorer qui disposent d'une version à jour. Les chercheurs jugent le processus de migration généralement lent, hormis pour Safari 3 vers lequel plus de 60% des utilisateurs de Safari avaient migré dans les trois mois qui ont suivi sa sortie. Cette mise à jour accélérée pourrait selon l'étude s'expliquer par la procédure (décriée) automatique intégrée à d'autres logiciels (dont iTunes) décidée par Apple.

Principaux vecteurs de courriers indésirables (spam), les bots seraient cent cinquante millions 150 000 000 selon Vinton Cerf, le co-inventeur de TCP/IP. Selon une autre estimation, entre 5 000 et 30 000 ordinateurs seraient transformés en PC zombies chaque jour. Lors de son dernier rapport, Symantec en décomptait 6 millions dans le monde, en hausse de 29% sur 6 mois.

Un réseau de machines zombies peut être constitué et contrôlé par une ou plusieurs personnes, afin d'obtenir une capacité considérable et d'avoir un impact plus important. Certains groupes de crackers en contrôleraient plusieurs centaines de milliers au sein de réseaux de zombies, qu'on appelle botnets à l'instar des réseaux de robots IRC du même nom. Ces botnets peuvent être utilisés pour commettre des délits comme le vol de données bancaires et identitaires à grande échelle. Les botnets sont plus à l'avantage d'organisations criminelles (mafieuses) que de pirates isolés, et peuvent être même loués à des tiers peu scrupuleux. Un réseau de machines zombies peut aussi être utilisé afin de fournir aux pirates une puissance de calcul phénoménale, leur permettant de déchiffrer un code en un temps considérablement plus court que sur une machine.

Le nombre de machines zombies dans un pays peut être évalué à partir de la provenance des courriers indésirables détectés. Le nombre de pourriels en provenance d'un pays par rapport à la quantité globale de pourriels détectés donne donc une indication du nombre de machines zombies d'un pays par rapport à l'ensemble des machines connectées sur le réseau.

Selon Sophos [ATT 08], début 2007, la première place a été attribuée aux États-Unis avec 22,0 %. La deuxième place était prise par la Chine (incluant Hong-Kong) avec 15,9 %, puis par la Corée du sud avec 7,4 %. La France était quatrième de ce palmarès avec 5,4 %, suivie de près par l'Espagne avec 5,1 % des pourriels détectés.

Après ce bref aperçu des attaques, menaces et dangers informatiques dans le monde, nous allons à présent nous concentrer sur une attaque spéciale qui consiste pour un intrus à s'introduire dans un système ou un réseau informatique étranger.

I.2.2 Le cas spécial des intrusions

Une intrusion est une forme particulière d'attaque informatique car la plupart des autres attaques servent souvent à préparer ou à rendre les cibles plus vulnérables afin de faciliter la réalisation des intrusions.

Les intrusions sont souvent effectuées dans les contextes d'espionnage industriel ou politique. Par exemple au tout début du mois d'octobre 2008 selon la rédaction du « Journal du Net », des pirates ont pu s'introduire dans le système informatique d'un fabricant sud-coréen de missiles et dérober des données. Selon le premier rapport de l'administration de la sécurité nationale du pays, le National Security Research Institute, les cyber-attaquants sont parvenus à installer un programme malveillant sur le réseau de l'industriel LIGNex1 Hyundai Heavy Industries.

Pour pouvoir mettre en œuvre 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.

L'obtention d'informations sur l'adressage du réseau visé, généralement qualifiée de prise d'empreinte, est souvent le 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.

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

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.

Lorsque le balayage du réseau est terminé, il suffit au pirate d'examiner les rapports 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 les versions des principales applications serveurs (Apache par exemple) dans les informations dites de « bannière ».

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

Lorsque le pirate a obtenu un ou plusieurs accès sur le réseau en se « logant » sur un ou plusieurs comptes peu protégés, celui-ci va chercher à augmenter ses privilèges en obtenant un accès root (en français superutilisateur), 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 renifler, 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. 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.

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.

Une fois la cartographie du système établie, le hacker 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 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).

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.

S'il s'agit d'un pirate expérimenté, 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 :

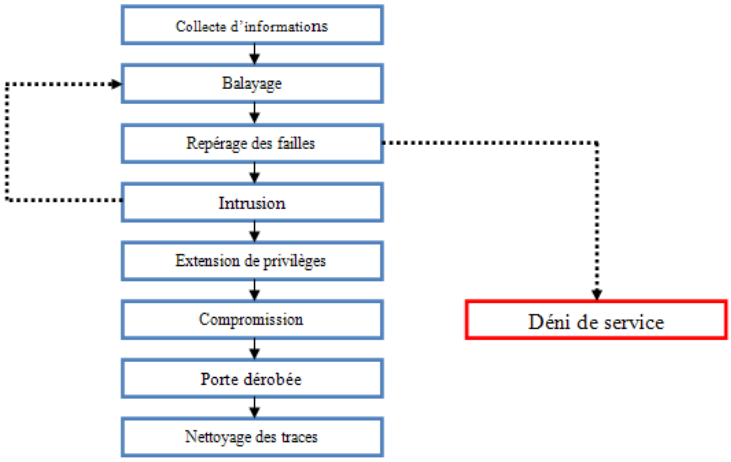


Figure 1-10 : Etapes de réalisation d'une intrusion informatique

La technique d'intrusion la plus répandue dans le monde numérique est celle réalisée à l'aide ou par les virus. En 1986 déjà, l'ARPANET fut infecté à cause de Brain, un virus qui renommait tous les disques de démarrage de système d'exploitation en (C)Brain. Les créateurs de ce virus y donnaient leur nom, adresse et numéro de téléphone car c'était une publicité pour eux.

Le champ d'application des virus va de la simple balle de ping-pong qui traverse l'écran au virus destructeur de données, ce dernier étant la forme de virus la plus dangereuse. Ainsi, étant donné qu'il existe une vaste gamme de virus ayant des actions aussi diverses que variées, les virus ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection. Ainsi on distingue ainsi plusieurs types de virus :

- les vers sont des virus capables de se propager à travers un réseau

- les troyens (chevaux de Troie) sont des virus permettant de créer une faille dans un système (généralement pour permettre à son concepteur de s'introduire dans le système infecté afin d'en prendre le contrôle)
- les bombes logiques sont des virus capables de se déclencher suite à un événement particulier (date système, activation distante, ...)

Il existe aussi des virus polymorphes qui, lors de leurs réplications, modifie leur représentation pour empêcher les anti-virus de les identifier par leur signature. Bien qu'en apparence ces virus changent, leur fonctionnement (leur méthode d'infection et leur charge utile) reste le même. Les algorithmes ne sont pas modifiés, mais leur traduction en langage machine l'est.

Comme le montre le graphe suivant, *Netsky* and *Nyxem* étaient les deux virus les plus répandus entre Mai et Juin 2008.

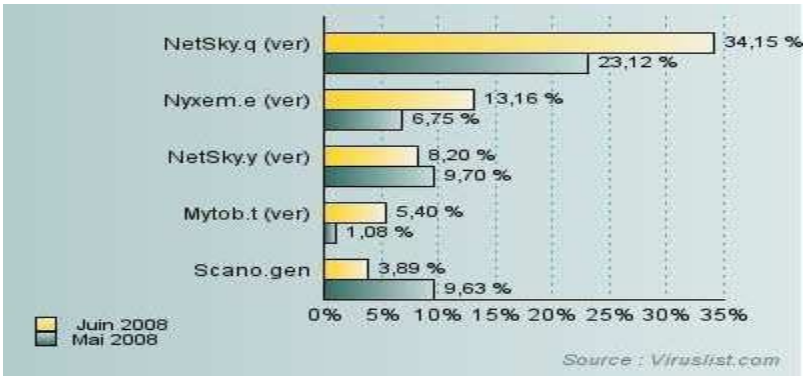


Figure 1-11 : Top 5 des virus en Juin 2008

Il y a aussi les espiogiciels (en anglais spyware) qui sont des programmes chargés de recueillir des informations sur les utilisateurs de l'ordinateur sur lequel ils sont installés (on les appelle donc parfois mouchards) afin de les envoyer à la personne qui les diffuse pour lui permettre de dresser le profil des internautes. Les informations recherchées sont souvent les mots-clés saisis dans les moteurs de recherche, les achats réalisés via internet, les URL des sites visités, les informations de paiement bancaire (numéro de carte bleue / VISA) etc.

Après avoir parlé brièvement des attaques informatiques en général et plus particulièrement des intrusions informatiques, nous allons à présent voir quelles sont les solutions et mesures de sécurité qu'il est possible actuellement de mettre en œuvre pour garantir un niveau satisfaisant de sécurité au sein des systèmes d'informations des entreprises et organismes.

I.3 Les solutions en matière de sécurité informatique

Les contrôles physiques n'assurent qu'une protection limitée des données et des ressources ; d'autres systèmes et outils comme ceux de la figure 1-12 sont primordiaux pour la réalisation de la sécurité logique des données et des ressources.

On retrouve dans ce graphe les antivirus et les pare-feu (firewall) en tête de liste du classement des mesures de sécurité les plus utilisées en 2007 selon les auteurs du rapport 2007 du Global Security Survey [GLO 07]. Toutes ces mesures de sécurité présentées dans ce graphe visent à garantir les services de sécurité que nous allons expliciter dans la sous section suivante.

Plus loin dans la troisième partie de ce document, nous nous intéresserons aux systèmes de surveillance et de protection contre les intrusions afin de mieux comprendre leur fonctionnement et les avantages qu'ils peuvent procurer aux entreprises dans une stratégie à long terme.

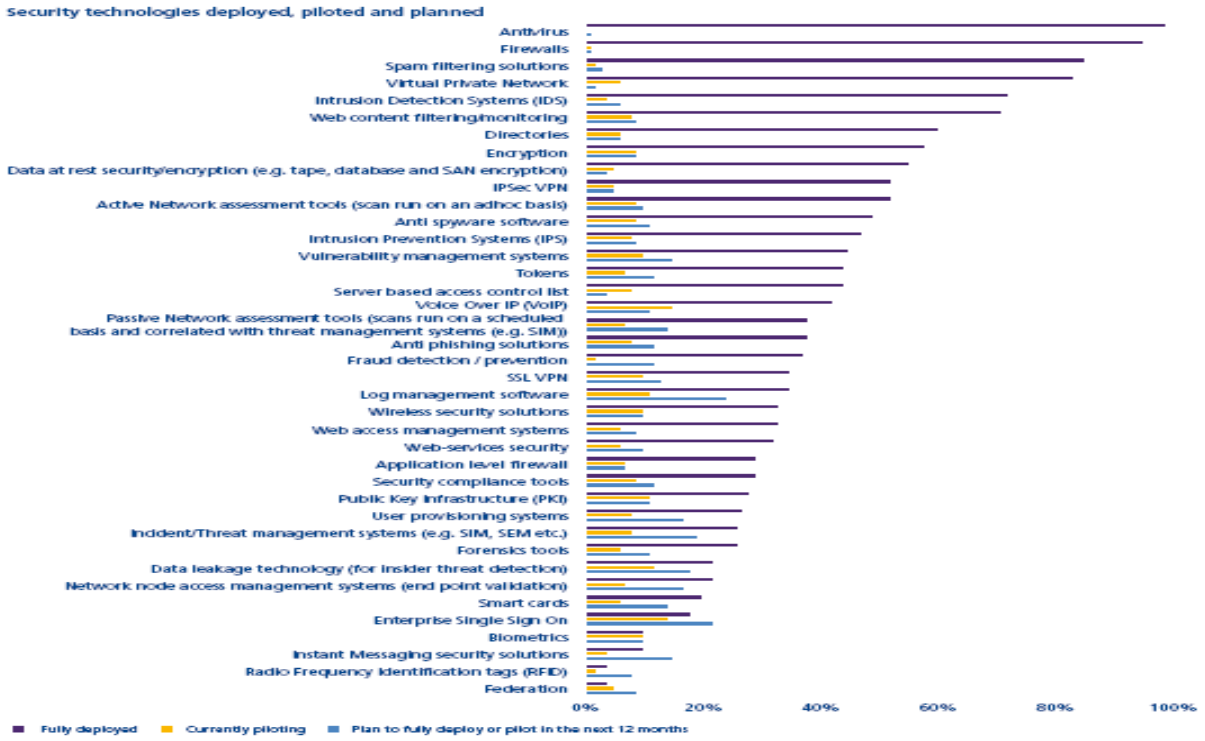


Figure 1-12 : Statistiques des systèmes de sécurité déployés en 2007

I.3.1 Les services et mécanismes de sécurité informatique

Les services de sécurité sont les critères principaux que doivent satisfaire les solutions de sécurité afin de garantir de manière méthodique et organisée la sécurité des systèmes et des réseaux. Il s'agit surtout de la disponibilité, l'intégrité, la confidentialité, l'authentification, l'autorisation, la non-répudiation, la traçabilité, l'auditabilité et le contrôle d'accès.

Le contrôle d'accès est un processus consistant à limiter les droits d'accès aux ressources du système. On peut citer trois types de contrôle d'accès :

- Les contrôles d'accès administratifs qui sont fondés sur les politiques générales. Les politiques de sécurité de l'information doivent énumérer les objectifs de l'organisation en matière de contrôle d'accès aux ressources, la prise de conscience des notions de sécurité, l'embauche et la gestion du personnel.
- Les contrôles logiques qui sont constitués des mesures matérielles et logicielles permettant de limiter l'accès au réseau, comme les listes de contrôle d'accès, les protocoles de communication et le chiffrement.
- Les contrôles physiques qui servent à empêcher tout accès physique non autorisé près des équipements ou près des salles qui contiennent le matériel critique constituant le réseau. Un des risques à ces bas niveaux est l'utilisation de renifleurs et d'analyseurs de paquets.

Le contrôle d'accès repose donc sur la vérification de l'identité (authentification), puis sur l'accord de privilèges selon l'identité en question (autorisation) et enfin sur le fait de ne pas pouvoir nier ou rejeter qu'un événement a eu lieu (Non répudiation).

Le contrôle d'accès consiste à vérifier si une entité (une personne, un ordinateur, …) demandant d'accéder à une ressource à les droits nécessaires pour le faire. Le contrôle peut être réalisé à l'aide de l'utilisation d'éléments permettant l'authentification de l'entité (par exemple un mot de passe, une carte, une clé, un élément biométrique, …). Des systèmes et protocoles comme Samba, Active Directory, LDAP et Radius permettent de gérer l'authentification souvent nécessaire aux contrôles d'accès logiques. Les mises en œuvre concrètes des solutions de contrôle d'accès sont les anti-virus, les pare-feux, les systèmes de détection et de prévention d'intrusion.

En ce qui concerne les mécanismes de sécurité, il s'agit en général des algorithmes ou des techniques cryptographiques qui permettent de fournir l'ensemble des services de sécurité cités ci-dessus. Il n'existe pas un simple mécanisme de sécurité qui fournisse l'ensemble des services de sécurité. Cependant, un élément particulier est à la base de la plupart des mécanismes de sécurité. Il s'agit du chiffrement.

Les systèmes de chiffrement font appel à des algorithmes de chiffrement souvent complexes qui modifient, à l'aide d'une clé de chiffrement plus ou moins longue, les caractères à protéger pour générer des données apparemment aléatoires. Le texte chiffré *(cyphertext)* peut alors être transmis sur un réseau non sécurisé. En effet, même s'il est intercepté, il ne pourra être compréhensible par un tiers qui ne possède pas la clé de déchiffrement permettant d'obtenir le texte initial en clair *(plaintext).*

La puissance de l'algorithme, la taille de la clé utilisée et la capacité à garder les clés secrètes de façon sécurisée déterminent la robustesse d'un système de chiffrement. L'algorithme n'a pas besoin d'être secret. Il est même recommandé qu'il soit public et publié afin que la communauté scientifique puisse tester sa résistance aux attaques et trouver les failles avant qu'un attaquant ne les exploite. Garder un algorithme secret ne renforce pas sa sécurité.

Un système de chiffrement est dit fiable, robuste, sûr ou sécurisé s'il reste inviolable indépendamment de la puissance de calcul ou du temps dont dispose un attaquant. Il peut être qualifié d'opérationnellement sécurisé si sa sécurité dépend d'une série d'opérations réalisables en théorie, mais irréalisables pratiquement (temps de traitement trop long en appliquant les méthodes de résolution connues et en utilisant la puissance de calcul disponible).

Il existe deux types de chiffrement :

- Chiffrement symétrique

Le système de chiffrement est qualifié de symétrique si, pour chiffrer ou déchiffrer un texte, il faut détenir une même clé pour effectuer ces deux opérations. L'émetteur et le récepteur doivent posséder et utiliser la même clé secrète pour rendre confidentielles des données et pour pouvoir les comprendre.

- Chiffrement asymétrique

Un système de chiffrement asymétrique est basé sur l'usage d'un couple unique de deux clés complémentaires, calculées l'une par rapport à l'autre. Cette paire de clé est constituée d'une clé publique et d'une clé privée. Seule la clé dite publique peut être connue de tous, tandis que la clé privée doit être confidentielle et traitée comme un secret. On doit connaître la clé publique d'un destinataire pour lui envoyer des données chiffrées. Il les déchiffrera à leur réception avec une clé privée qu'il est le seul à connaître. Le message est confidentiel pour le destinataire dans la mesure où lui seul peut le déchiffrer.

I.3.2 Classification et principes des mesures de sécurité

Les mesures de sécurité se distinguent (figure 1-13) et se classifient selon leur niveau d'intervention. Elles contribuent toutes à protéger les ressources critiques de menaces particulières. Plusieurs types génériques de mesures de sécurité sont identifiés :

- Les mesures structurelles, comme l'occultation des ressources, les redondances, la fragmentation de l'information, par exemple, qui réduisent la vulnérabilité des ressources en agissant sur la structure et l'architecture du système d'information.
- Les mesures de dissuasion qui autorisent une prévention en décourageant les agresseurs de mettre à exécution une menace potentielle. Il peut s'agir de procédures juridiques et administratives touchant à la sensibilisation et à la gestion des ressources humaines, aux conditions de travail ou aux moyens de détection et de traçage.
- Les mesures préventives qui servent de barrière afin d'empêcher l'aboutissement d'une agression (incident, malveillance, erreur, etc.) et font en sorte qu'une menace n'atteigne pas sa cible. Les procédures de contrôles d'accès physique et logique, les détecteurs de virus, entre autres, peuvent jouer ce rôle.
- Les mesures de protection qui ont pour objectifs de réduire les détériorations consécutives à la réalisation d'une menace. En particulier, les contrôles de cohérence, les détecteurs d'intrusion, d'incendie, d'humidité, d'erreurs de transmission, et les structures coupe-feu permettent de se protéger des agressions ou d'en limiter l'ampleur.
- Les mesures palliatives ou correctives, telles que les sauvegardes, les plans de continuité, les redondances, les réparations ou corrections par exemple, qui pallient ou réparent les dégâts engendrés.

Les mesures de récupération qui limitent les pertes consécutives à un sinistre et réduisent le préjudice subi par un transfert des pertes sur des tiers (assurance) ou par attribution de dommages et intérêts consécutifs à des actions en justice.

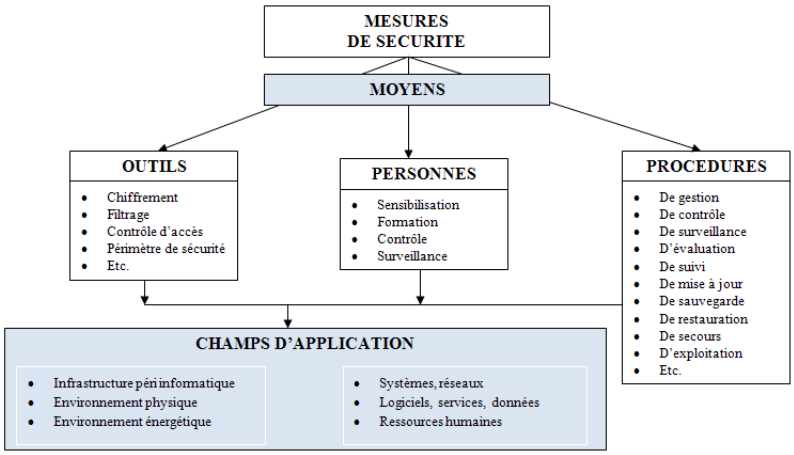


Figure 1-13 : Eléments constitutifs et champs d'application des mesures de sécurité

Il existe 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.

- CERT IST dédié à la communauté Industrie, Services et Tertiaire française,
- CERT IST dédié à l'administration française,
- CERT Renater dédié à la communauté des membres du GIP RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche).

Au niveau des mesures de sécurité aussi des évolutions ont été observées. En prenant par exemple le cas des pare-feux, les tout premiers étaient dits « stateless » ou sans état. Un pare-feu sans état regarde chaque paquet indépendamment des autres et le compare à une liste de règles préconfigurées.

La deuxième génération de pare-feu est le pare-feu à états ou « statefull ». Certains protocoles dits « à états » comme TCP introduisent la notion de connexion. Les pare-feu à états vérifient la conformité des paquets à une connexion en cours.

La troisième génération de pare-feu est le pare-feu applicatif. Dernière véritable 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 HTTP passe par le port TCP 80.

La quatrième génération de pare-feu est le pare-feu identifiant. Un pare-feu identifiant 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 IP, et suivre l'activité réseau par utilisateur.

La cinquième génération de pare-feu est le pare-feu personnel. Les pare-feux personnels généralement installés sur une machine de travail, agissent comme un pare-feu à états. Il s'agit en fait de nouveaux antivirus qui intègrent des pare-feux. Aujourd'hui, toutes ces évolutions des pare-feux ont conduit à une situation telle qu'il n'est plus aisé de différencier les effets d'un pare-feu classique et ceux d'un antivirus.

Après les pare-feux sont apparus les concepts de réseaux privés virtuels (VPN). Ensuite ce fut le tour des systèmes de détection et de prévention d'intrusions. Ces systèmes qui sont réputés être plus fiables que les pare-feux seront analysés et décortiqués dans la troisième partie de ce document car ils viennent en réponses aux attaques ciblées qui se manifestent souvent sous la forme d'intrusions informatiques.

Etant donné l'augmentation des menaces combinées, du spam et des attaques de phishing, il n'a jamais été aussi important de communiquer à l'utilisateur quels sont les meilleurs moyens de se protéger.

Une éthique sécuritaire doit être développée au sein de l'entreprise pour tous les acteurs du système d'information. Elle doit se traduire par une charte reconnue par chacun et par un engagement personnel à la respecter. La signature de la charte de sécurité doit s'accompagner des moyens aux signataires afin qu'ils puissent la respecter.

De plus, il est également nécessaire d'éduquer, d'informer et de former aux technologies de traitement de l'information et des communications et non uniquement à la sécurité et aux mesures de dissuasion. La sensibilisation aux problématiques de sécurité ne doit pas se limiter à la promotion d'une certaine culture de la sécurité et de son éthique. En amont de la culture sécuritaire, il doit y avoir une culture de l'informatique ce qui correspond à la notion de permis de conduire informatique que prône le Cigref (Club informatique des grandes entreprises françaises dont le site Internet est www.cigref.fr).

L'audit est une procédure de contrôle de la gestion d'une activité et de l'exécution de ses objectifs. En matière de systèmes d'information, l'audit de sécurité a pour objectif de mesurer l'écart entre la situation existante (sur les plans organisationnels, procéduraux et techniques) et la politique de sécurité de l'entreprise, les bonnes pratiques et l'état de l'art.

Un audit de sécurité doit conduire, au delà du constat, d'une part à mesurer les risques opérationnels pour le domaine étudié, et par extension pour toute ou partie des activités de l'entreprise, et d'autre part à proposer des recommandations et un plan d'actions quantifiées et hiérarchisées pour corriger les vulnérabilités et réduire l'exposition aux risques.

Les audits font intervenir :

- Soit une équipe pluridisciplinaire d'experts interne à l'entreprise ;
- Soit une équipe pluridisciplinaire composée de consultants et d'ingénieurs (experts dans leurs domaines) externes à l'entreprise.

Les tests d'intrusion (en anglais « penetrations tests », abrégé en pen tests) consistent à éprouver les moyens de protection d'un système d'information en essayant de s'introduire dans le système en situation réelle.

On distingue généralement deux méthodes distinctes :

- La méthode dite « boîte noire » (en anglais « black box ») consistant à essayer d'infiltrer le réseau sans aucune connaissance du système, afin de réaliser un test en situation réelle ;
- La méthode dite « boîte blanche » (en anglais « white box ») consistant à tenter de s'introduire dans le système en ayant connaissance de l'ensemble du système, afin d'éprouver au maximum la sécurité du réseau ;

Un test d'intrusion, lorsqu'il met en évidence une faille, est un bon moyen de sensibiliser les acteurs d'un projet. A contrario, il ne permet pas de garantir la sécurité du système, dans la mesure où des vulnérabilités peuvent avoir échappé aux testeurs. Les audits de sécurité permettent d'obtenir un bien meilleur niveau de confiance dans la sécurité d'un système étant donné qu'ils prennent en compte des aspects organisationnels et humains et que la sécurité est analysée de l'intérieur.

A présent, nous allons passer à l'état des lieux de la sécurité informatique dans le monde.

I.4 Etat des lieux de la sécurité informatique dans le monde

Pour mieux prendre conscience de la problématique de la sécurité informatique et de l'Internet, les chercheurs se basent souvent sur des études, recherches de laboratoire, enquêtes et constats des centres spécialisés dans la collecte des informations concernant l'informatique et son évolution.

Le Computer Crime and Security Survey (CCSS-CSI) réalise chaque année un des sondages les plus pertinents aux Etats-Unis au sujet des problèmes menaçant la sécurité informatique. Elle mène ses recherches auprès des organismes gouvernementaux, institutions civiles, multinationales, universités, hôpitaux etc. Le 12ème sondage annuel du CSI en collaboration avec le Federal Bureau of Investigation (FBI) a fourni des chiffres et statistiques alarmants sur l'état de la sécurité informatique et de l'Internet en ce qui concerne l'année 2007.

Le Global Security Survey, une autre étude non moins intéressante émane du « It Risk Management And Security Services » du Groupe « Global Financial Services Industry (GFSI)». Ce groupe appartient au cabinet d'audit et de conseil britannique « Deloitte Touche Tohmatsu (DTT) ». Les domaines d'activité de cette multinationale sont l'audit, le juridique, la finance, l'expertise comptable, la certification, la fiscalité, la consultation en gestion et les conseils financiers. Il possède plus de 150 000 collaborateurs dans le monde avec un chiffre d'affaire s'élevant à 23,1 milliards de dollars pour l'exercice 2006-2007. Ce groupe est présent à travers 69 firmes dans 142 pays à travers le monde.

Le Club de la Sécurité de l'Information Français (CLUSIF) aussi réalise chaque année un rapport intitulé « les menaces et les pratiques de sécurité ». Le rapport 2008 du CLUSIF a concerné 354 entreprises de plus de 200 salariés, 194 collectivités locales et 1139 individus issus du panel d'internautes de l'institut spécialisé Harris Interactive.

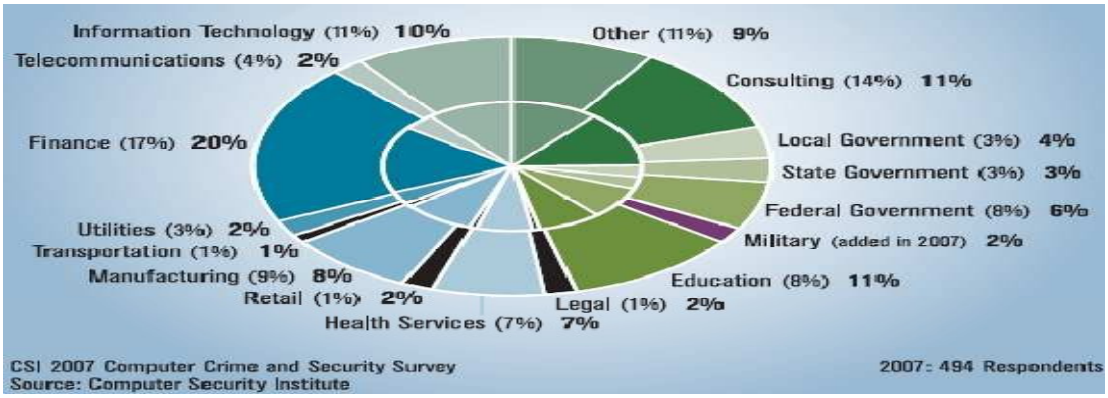
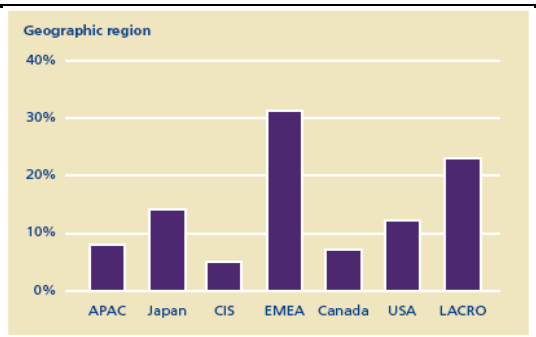


Figure 1-14 : Statistiques des réponses par secteur d'activité

Tandis que les sondages du CSI et du CLUSIF se focalisent sur une population très diversifiée mais limitée respectivement aux Etats-Unis (figure 1-14) et en France, le sondage du GFSI s'intéresse plutôt aux institutions financières comme les banques et les firmes d'assurance dans le monde entier (figures 1-15 et 1-16).



- Asia Pacific (APAC) (excluding Japan) – 8%.
- Japan – 14%.
- Former Soviet Republics – Commonwealth of Independent States – (CIS) – 5%.
- Europe, the Middle East and Africa (EMEA) – 31%.
- Canada – 7%.
- USA – 12%.
- Latin America and the Caribbean (LACRO) – 23%.

Figure 1-15 : Statistiques des réponses par situation géographique

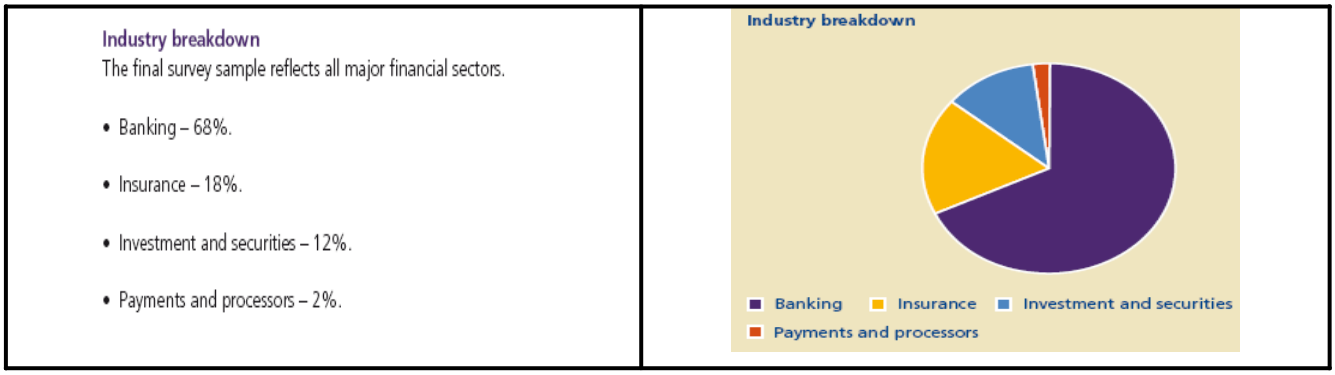


Figure 1-16 : Secteurs d'activités des entreprises ayant participé au sondage

Après une analyse approfondie des résultats de ces trois sondages, le premier constat que nous pouvons faire est que l'ensemble des attaques portées contre les systèmes et les réseaux informatiques des entreprises et des organisations leur causent des pertes financières considérables et d'énormes dommages en ce qui concerne leur image et leur réputation (le cas des dénis de service).

En analysant le graphique de la figure 1-17 tiré du rapport du CSI, rien qu'aux Etats-Unis, on estime les pertes causées par les fraudes financières à $21 124 750 et $8 391 800 en ce qui concerne les virus et les spywares. Tout ceci rien qu'en 2007. Les fraudes financières ont donc pris la première place qui était occupé par les virus.

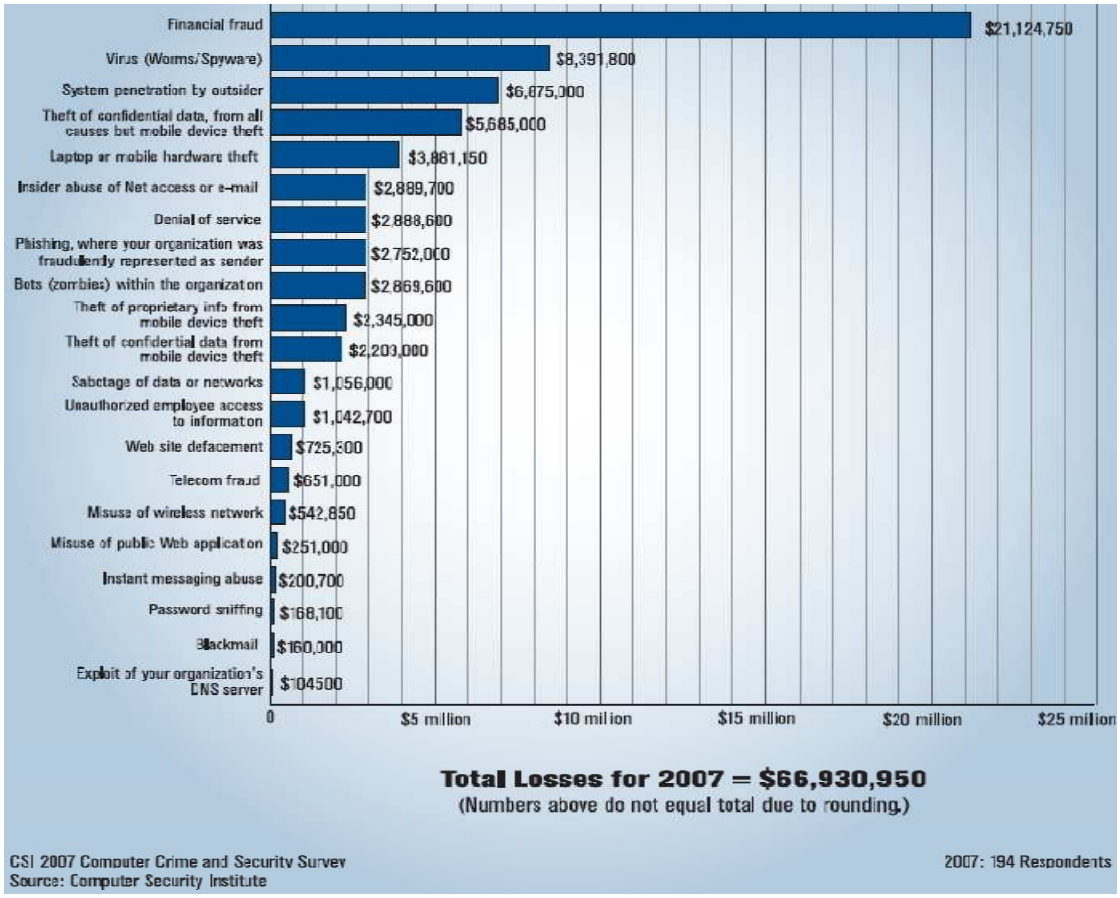


Figure 1-17 : Statistiques des pertes financières (en dollars US) par types d'attaques

Les auteurs du rapport du CSI ont estimé que les pertes financiers causées par les divers types d'incidents de sécurité ont connu une baisse progressive ces cinq dernières années y compris en l'an 2006 mais pas pour l'année 2007. En effet, le totale des pertes en 2007 (même si le

nombre de personnes ayant répondu à cette question relative aux pertes a diminué : 194) a été estimé à $66 930 950 ce qui est une hausse significative car en 2006 ce total était de $52 494 290 pour 313 réponses obtenues.

La meilleure manière d'apprécier ces pertes financières est de les voir sous forme de moyenne des pertes par personne interrogée (organisme ou représentant ayant participé au sondage) et c'est justement ce que montre la figure 1-18. Cette année, la moyenne des pertes par personne interrogée est de $345 005 ce qui représente une très forte hausse par rapport au résultat de l'an 2006 qui était de $167 713.

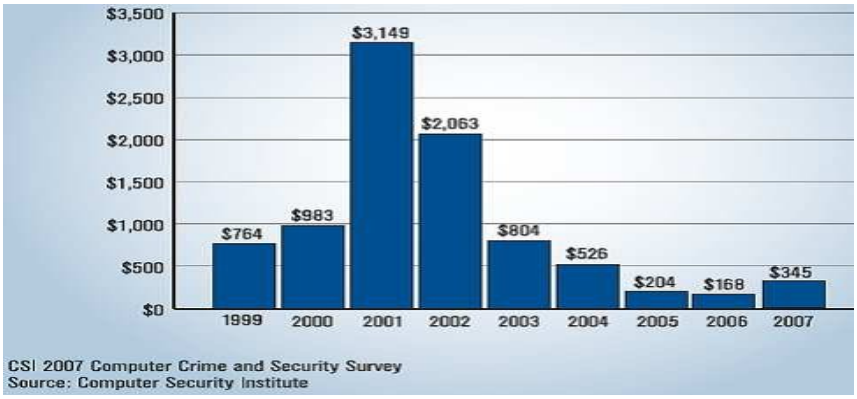


Figure 1-18 : Moyennes des pertes financières (en dollars US) par organismes sondés.

Les mesures de sécurité prises en général par les organisations contre les attaques sont basées sur des composants et logiciels comme les antivirus et les pare-feux qui ne sont fondamentalement pas parfait en raison de l'évolution quasi quotidienne des menaces informatiques. Cela est dû en grande partie au fait que ces technologies se basent sur la détection par des signatures. Cette approche par recherche de signature des menaces connues n'est pas toujours très pratique car les concepteurs de logiciels malveillants (virus et autres) ont progressivement augmenté la sophistication de leurs outils à un point tel qu'il leur est possible d'outre passer les anti-virus quasiment à volonté (selon les auteurs de la première étude). Certes c'est souvent pour un court moment (le temps que les concepteurs d'antivirus réagissent) mais ces courts moments sont souvent suffisants pour ces malfaisants pour réaliser leurs méfaits.

L'usage de l'informatique et d'Internet à la maison est maintenant largement banalisé. Le comportement des utilisateurs de l'informatique en entreprise est de plus en plus souvent influencé par la pratique privée, et les frontières entre les deux mondes deviennent plus floues. L'enquête du CLUSIF montre qu'un tiers des internautes utilisent l'ordinateur familial aussi à des fins professionnelles (figure 1-19), ce qui pose quelques questions sur la protection des données de l'entreprise… Et si les internautes sont globalement prudents dès qu'il s'agit d'achat sur Internet, et semblent conscients de l'utilité des outils de protection (antivirus, pare feu personnels, etc.), ils ne se sentent que pour une minorité d'entre eux véritablement en « insécurité » sur Internet.

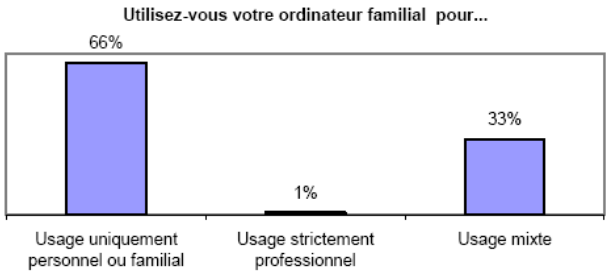


Figure 1-19 : Types d'usage de l'ordinateur familial

Pendant que les logiciels malveillants deviennent de plus en plus sophistiqués, les systèmes d'exploitation actuels deviennent de plus en plus complexes, comportant ainsi une infinité de vulnérabilités. Il suffit de consulter les bulletins d'information des CERT pour constater qu'on en découvre quasiment tous les jours.

Dans ce contexte où les virus, les chevaux-de-Troie et les autres logiciels malveillants deviennent de plus en plus sophistiqués, on assiste à la recrudescence d'un type d'attaques qui était encore il y a cinq ans seulement évoqués dans les débats théoriques sur la cybercriminalité. Aujourd'hui cela devient une réalité si on en croit la figure 1-20 :

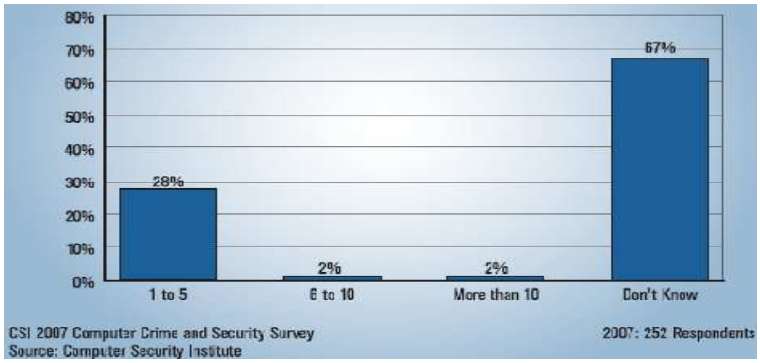


Figure 1-20 : Statistiques des organisations ayant été victimes d'attaques ciblées

Il s'agit des attaques ciblées. Selon les auteurs du sondage 2007 du CSI, ce n'est qu'en cette année (2007 : année du rapport actuel, c'est-à-dire le rapport le plus récent du CSI car celui de 2008 sortira en début 2009) que cette question a été ajoutée dans les formulaires du sondage. 32% de ceux qui ont répondu à cette question estiment avoir effectivement essuyés ce type d'attaque (figure 1-20). Les attaques ciblées sont plus difficiles à détecter que les attaques génériques et conventionnelles que subit l'ensemble de la communauté des utilisateurs des ressources informatiques. C'est pourquoi elles sont plus dangereuses car les systèmes visés la plupart du temps ne s'en rendent même pas compte (ou elles s'en rendent compte parfois bien longtemps après). Etant donné que les attaques ciblées réussissent le plus souvent à atteindre leurs objectifs, si les criminels qui le font sont attirés par l'appât du gain, il est fort possible que dans les prochains rapports du CSI et du GFSI, on en dénombrera encore beaucoup plus.

Par ailleurs, la demande croissante de mobilité et d'interopérabilité des fonctions informatiques et de la sécurité a progressivement conduit à une grande variété de moyens de communication. Toutes ces méthodes et techniques apportent bien sûr elles aussi leurs lots de risques en matière de sécurité informatique. Les auteurs du rapport du Global Security Survey [GLO 07] rapportent ainsi que 77% des personnes et organismes interrogés ont indiqués qu'ils avaient fait l'expérience de plusieurs cas répétés de découvertes de brèches de sécurité dans leurs réseaux ou systèmes informatiques.

Il n'est déjà pas bon signe de déceler des brèches dans son système de sécurité mais quand une ou plusieurs mêmes brèches réapparaissent plusieurs fois de suite (découverte, fermeture ensuite redécouverte), cela devient un sérieux risque pour l'entreprise ou l'organisation et il y a lieu de vraiment s'inquiéter et d'approfondir les investigations.

Les brèches de sécurité causées par les virus et les chevaux-de-Troie sont souvent plus fréquents que ceux causées par les employés tant intentionnellement qu'accidentellement. Le tableau de la figure 1-22 montre un aperçu général des réponses obtenues en ce qui concerne les brèches causées par des facteurs externes. Il est particulièrement inquiétant de constater

que pour l'année 2007, les attaques par e-mail (spams et spyware) ont pris la première place dans la liste avec 52% des personnes interrogées qui ont rapportés les avoir subit.

En ce qui concerne les brèches créées par des facteurs internes aux organismes (tableau 1-1), il est heureux de constater que les incidents du genre virus, vers ou fraudes financières ont largement baissés ces trois dernières années. De 31% en 2005, on est passé à 28% en 2006 puis à 18% en 2007. Toutefois les cas d'accidents (13%) et de pertes des données privées des clients (8%) ont été signalés pour la première fois dans le rapport de cette année selon le tableau 1-2.

Internal breach Experience	One Occurrence (%)	Repeated Occurrence (%)
Virus/Worm outbreaks	8	13
Wireless network breach	1	0
Loss of customer data/privacy issues	4	8
Internal financial fraud involving information system	7	11
Theft or leakage of intelligence property (e.g. customer leakage)	3	7
Accidental instances	5	13
Other form of internal breach	2	10
Do not know	3	2

Tableau 1-1 : Statistiques des brèches de sécurité provenant des sources internes aux organisateurs

External breach Experience	One Occurrence (%)	Repeated Occurrence (%)
Virus/Worm outbreaks	11	40
Email attacks (i.e. spam)	5	52
Spyware	6	26
Zombie networks	2	6
Denial of service	7	8
Web site defacement	2	2
Malicious remote access	4	4
Online extorsion	1	1
Wireless network breach	1	1
Phishing/Pharming	5	35
Social engineering	5	17
Employee misconduct	8	31
Theft or leakage of intelligence property	5	8
External financial fraud involving information system	5	13
Exposure of sensitive data through web attacks	1	1
Physical threats	8	10
Accidental instances	4	14
Other form of external breach	3	2
Do not know	3	4

Tableau 1-2 : Statistiques des brèches de sécurité provenant des sources internes aux organisateurs

Selon les auteurs du sondage du GFSI, parmi les dommages occasionnés par ces brèches, 58% sont des pertes financières directes, 30% des pertes indirectes et 12% des pertes sont touchent négativement à la réputation des entreprises.

Les auteurs du sondage GFSI soulignent aussi le fait qu'à la question de savoir si leur organisation va au-delà de l'authentification par des mots de passe pour réaliser les transactions sur Internet avec leurs clients, un peu plus de la moitié (51%) ont répondu par l'affirmative tandis que 14% et 7% ont répondu être sur le point de le faire respectivement dans les 12 et 24 mois prochains.

Quant à la question de savoir si un événement anormal (des événements autre que ceux du type analyse complète et rapide du réseau par des sniffers) a été constaté, 46% des personnes sondées ont répondu par l'affirmative selon les auteurs du rapport 2007 du sondage du CSI. Ce pourcentage est en baisse par rapport au 52% de l'année 2006, au 56% de l'année 2005 et surtout au pic de 70% de l'an 2000.

Dans le même sens, il a été demandé aux personnes sondées d'estimer le nombre d'incidents qu'ils auraient essuyés durant les 12 derniers mois (2007). La figure 1-21 indique que le nombre d'incidents détectés a significativement augmenté surtout en ce qui concerne la tranche de ceux qui ont estimé avoir subit plus de 10 attaques (de 9 à 26%).

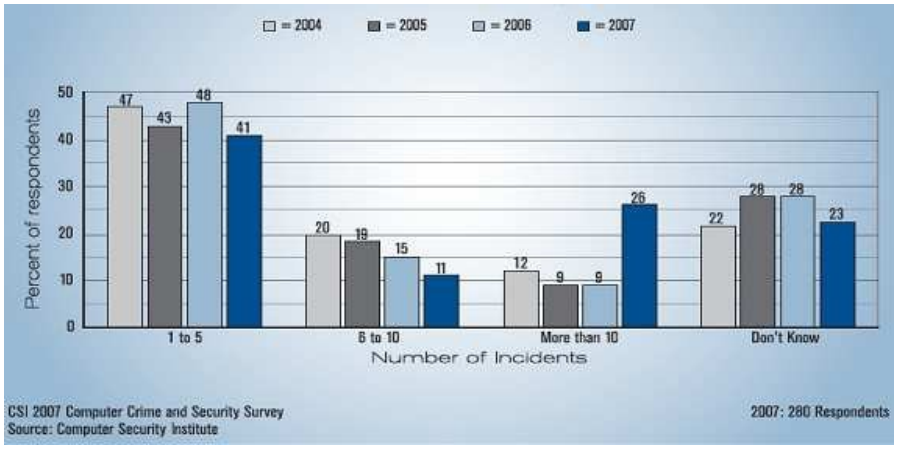


Figure 1-21 : Statistiques du nombre d'incidents subit ces 12 derniers mois par les organisations.

La figure 1-22 montre le pourcentage des attaques provenant de l'intérieur même des entreprises et des organisations aux Etats-Unis. Comme on peut le voir, 27% des personnes sondées attribuent moins de 20% de leurs pertes financières aux menaces internes. 37% des personnes interrogées estiment le pourcentage de leurs pertes attribuées aux menaces internes entre 20 et 40%. Et seulement 5% de la population sondée attribue plus de 80% de leurs pertes aux menaces internes.

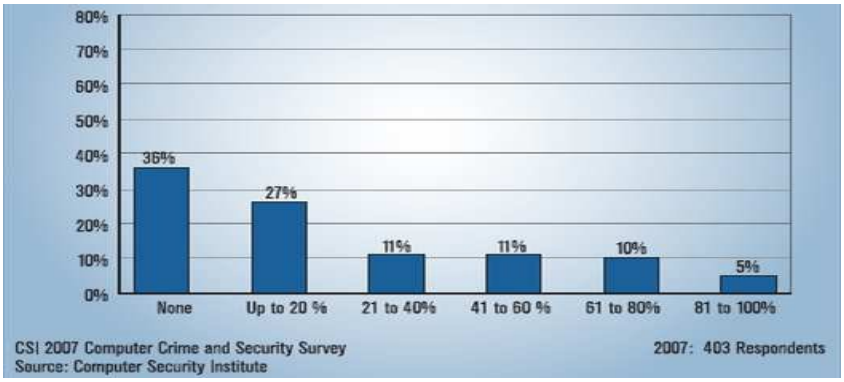


Figure 1-22 : Pourcentage des pertes dues aux facteurs internes (le personnel) de l'entreprise.

En ce qui concerne les entreprises, l'édition 2008 du rapport du CLUSIF fait ressortir un inquiétant sentiment de stagnation. Entre 2004 et 2006 des progrès notables avaient été fait, en particulier dans le domaine de la formalisation des politiques et des chartes de sécurité. Mais depuis, il semble bien que la mise en application concrète de ces politiques soit restée un vœu pieu. 40 % des entreprises ne disposent toujours pas de plan de continuité d'activité pour traiter les crises majeures, contre 42 % en 2006 (figure 1-23). Et 30 % d'entre elle disent ne pas être en conformité avec la Loi Informatique et Liberté…

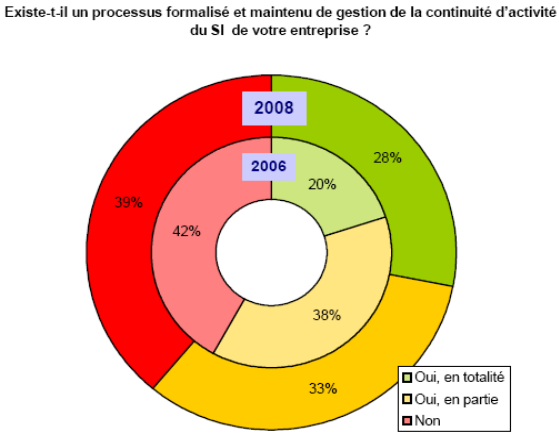


Figure 1-23 : mise en place d'un processus de gestion de la continuité d'activité du SI

Selon le diagramme issu de la figure 1-24 du rapport du CLUSIF, 59 % des entreprises disent réaliser une veille systématique ou partielle sur les nouvelles failles de sécurité et sur les nouvelles attaques.

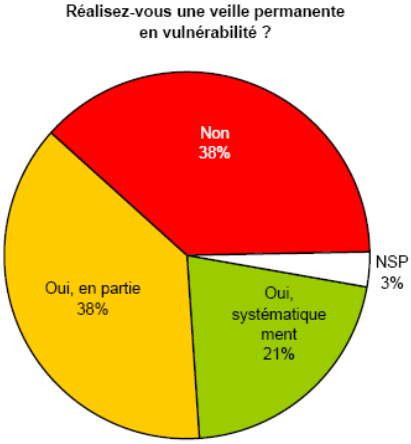


Figure 1-24 : Réalisation d'une veille permanente en vulnérabilité

Les grandes entreprises déclarent plus souvent réaliser une veille systématique, c'est-à-dire couvrant très largement le périmètre de leurs environnements techniques. Ce chiffre reste à peu près stable par rapport à 2006. Les entreprises n'ont globalement pas renforcé leur vigilance vis-à-vis des menaces.

Selon les auteurs de [CSI 07], toutes les catégories d'attaques ont tendance à diminuer en nombre depuis quelques années. Pourtant, pour l'année 2007, une hausse a été constatée en ce qui concerne par exemple les abus liés au personnel interne des entreprises (Insider abuse of network access or email) comme les visites des sites web pornographiques ou l'utilisation des logiciels piratés. De 42% en 2006 on est passé à 59%. En outre, pour le vol des ordinateurs portables et autres accessoires mobiles, on déplore aussi une légère hausse de 47% à 50%.

En ce qui concerne le pourcentage des entreprises ou organismes ayant subit des incidents sur leur site web, la figure 1-25 parle d'elle même. 40% des organismes interrogés estiment avoir essuyé entre 1 et 5 incidents de ce type.

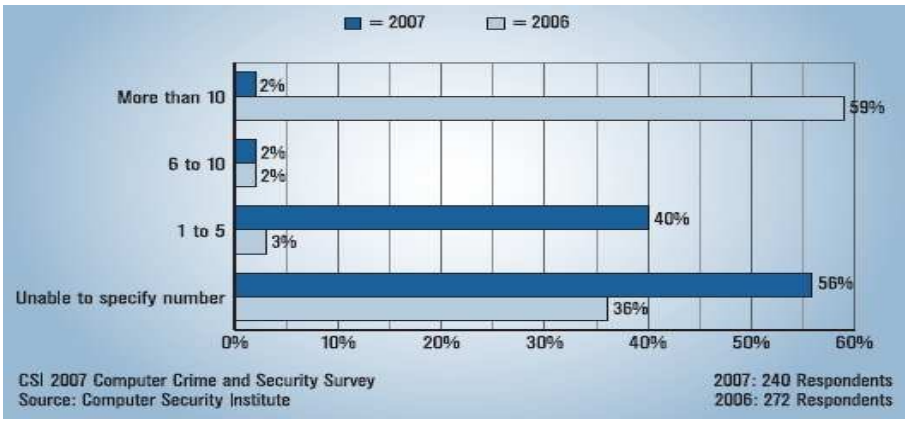


Figure 1-25 : Pourcentage des entreprises ou organisations ayant subit des attaques sur leur sites web.

Selon les auteurs du rapport du CSI de 2007 [CSI 07], le pourcentage des organisations qui ont rapporté des intrusions dans leurs réseaux ou systèmes informatiques continue d'augmenter après avoir connu une longue période de baisse (due certainement au manque de confiance dans les CERT autour des années 2000). Cette année, 29% des organisations qui ont participé au sondage disent avoir informé les institutions comme les CERT. C'est une légère hausse par rapport à 2006 (25%). La figure 1-26 montre justement le pourcentage des actions et mesures de sécurité prises en général suite à une attaque ou à un incident de sécurité.

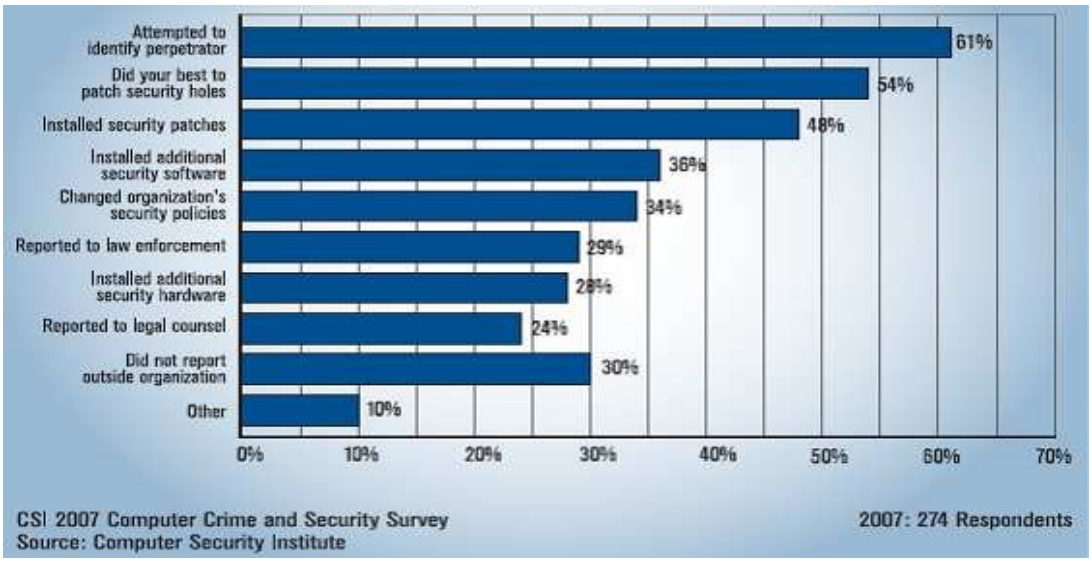


Figure 1-26 : Pourcentage des mesures ou actions prises suite à un incident.

De grosses lacunes dans la compréhension des situations à risque ont été constatées par les auteurs du rapport du CLUSIF. Pour les internautes interrogés sur les comportements et les situations à risque, l'absence de protections vis-à-vis des menaces virales arrive logiquement en première place (figure 1-27).

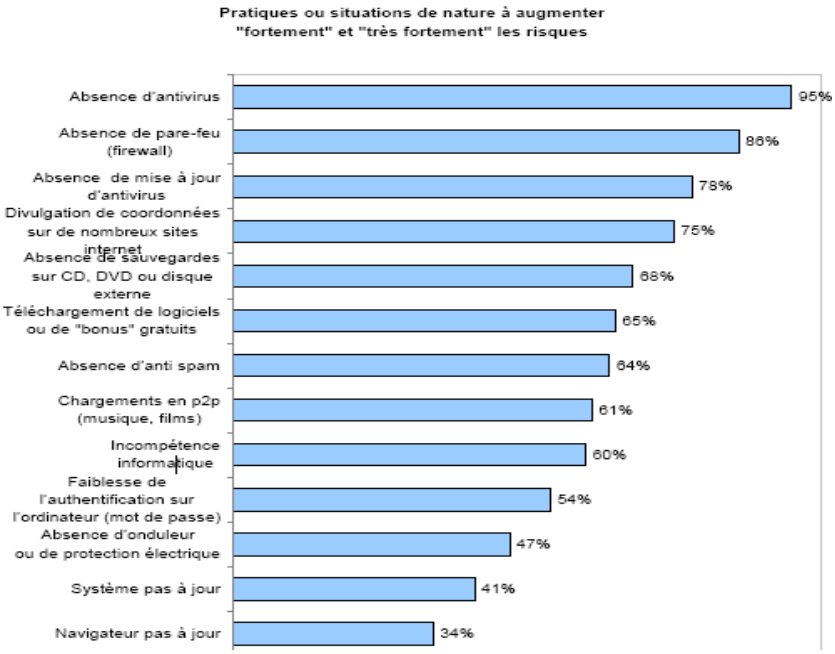


Figure 1-27 : pratiques et situations jugées à risque par les internautes

Nous devons noter le besoin d'éducation et de sensibilisation aux bonnes pratiques des utilisateurs qui considèrent majoritairement que ne pas mettre à jour leurs systèmes et navigateurs n'augmente pas fortement les risques, alors qu'en pratique, c'est primordial. Un système d'exploitation pas à jour, même doté d'un antivirus, sera la plupart du temps vulnérable aux attaques externes.

Pour conclure leur rapport, les experts du CLUSIF [MEN 08] ont affirmé que : « … *la menace ne faiblit pas et notre enquête montre de nouveau que les malveillances et les incidents de sécurité sont bien réels, avec une présence toujours active des attaques virales, des vols de matériel, et un accroissement des problèmes de divulgation d'information et des attaques logiques ciblées. Et l'actualité récente n'a cessé de démontrer les graves impacts des déficiences en matière de sécurité (fraude bancaire, divulgation de données personnelles, etc). Sortir des politiques de sécurité « alibi », que l'on rédige pour se donner bonne conscience, pour aller vers des pratiques concrètes, réellement ancrées dans les processus de gestion de l'information, voilà donc l'enjeu pour les années à venir…* »

Quant aux auteurs des deux autres rapports [GLO 07], [CSI 07], ils s'accordent pour dire que même s'il est mal de projeter la tendance des résultats d'une seule année aux années prochaines, il y a néanmoins une forte suggestion exprimant que les menaces émergentes commencent à se matérialiser en des pertes financières en forte croissance. Ils s'accordent aussi à dire que les nouvelles menaces prennent de l'ampleur (les attaques ciblées par exemple).

Gartner [CSI 07] a estimé que le revenu mondial des logiciels de sécurité est monté à $7,4 milliards en 2005, une augmentation de 14,8% du revenu de 2004 qui s'élevait à $6,4 milliards; $4 milliards de ce montant constituait le revenu généré par les logiciels anti-virus. En d'autres termes, l'identification des modèles de virus comptait pour 54,3% de toute l'industrie des logiciels de sécurité. En outre, les logiciels anti-virus ne sont pas les seuls outils de sécurité qui utilisent la recherche basée sur les signatures. La plupart des logiciels et matériels de pare-feu fonctionnent selon le même principe, pourtant ces techniques de recherche par signatures deviennent insuffisants notamment contre les attaques ciblées. Les

pirates améliorent leurs logiciels et outils malveillants à un point où la détection par des signatures n'est plus aussi efficace qu'à ses débuts.

L'un des problèmes majeures auquel le monde des technologies fait face actuellement est que les systèmes d'exploitation, les applications et les logiciels qui sont développés aujourd'hui utilisent des technologies et des composants tellement complexes (souvent sous le prétexte d'un meilleur design) qu'ils regorgent malheureusement de multiples vulnérabilités que les CERT découvrent et publient quasiment chaque jour. Pendant ce temps, les criminels informatiques conçoivent des logiciels et outils de plus en plus sophistiqués. Ainsi, pendant que les pirates disposent d'armes de plus en plus performantes, les grandes firmes informatiques (Microsoft et autres) leur offrent sur des plateaux des cibles parfaites que sont les utilisateurs finaux (organisations, entreprises et particuliers).

Dans le passé, la lutte au sujet de la sécurité informatique avait lieu entre les professionnels de la sécurité des entreprises et les criminels qui attaquaient leurs réseaux. Aujourd'hui c'est devenu encore plus compliqué. Les criminels attaquent à la fois les réseaux des entreprises et les données personnelles des clients de ces entreprises. C'est-à-dire qu'ils volent ces données au sein des entreprises et les emploient après pour attaquer les différents clients.

Un autre constat est que l'ensemble des firmes de hautes technologies semble se concentrer sérieusement sur la rénovation des systèmes de gestion d'identité (figure 1-28).

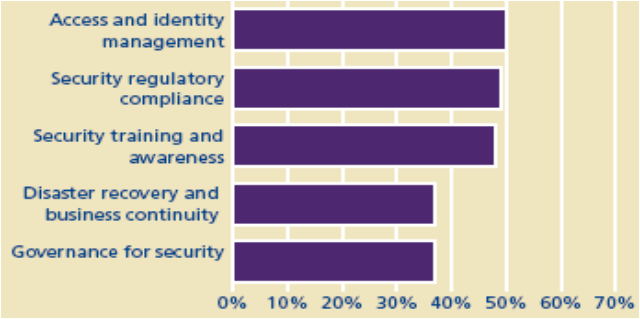


Figure 1-28 : Top 5 des initiatives prises en faveur de la sécurité informatique en 2007.

C'est une tendance qui, si elle réussit, pourrait très bien court-circuiter cette recrudescence de cyber crimes que nous constatons depuis les années 2000. En effet, il sera beaucoup plus difficile d'utiliser des astuces informatiques pour commettre des crimes en ligne si les utilisateurs sont obligés de s'authentifier sans équivoque, en employant des identifiants plus fiables que des adresses e-mail. Lorsqu'ils commettront des infractions, il sera alors facile de retrouver leurs noms et adresses dans le monde réel. C'est pourquoi les entreprises qui ont participé au sondage du GFSI ont mis en tête de leur liste de priorités la rénovation de leur système de gestion d'identités comme le montre la figure 1-28.

Une gestion d'identité plus rigoureuse (en particulier avec des protections plus appropriées de la vie privée) pourrait être une bonne carte à jouer pour les entreprises (d'autres entreprennent également les révisions de leurs applications pour les rendre moins vulnérables) qui désireraient se libérer de la menace ou de l'emprise des pirates.

Arrivés à la fin de cette première partie, nous comprenons clairement que la situation de la sécurité informatique est tout de même inquiétante. Comme nous le disions un peu plus haut, pendant que les cybercriminels deviennent de plus en plus nombreux et que des outils permettant de mener des attaques informatiques deviennent de plus en plus disponibles en libre téléchargement sur Internet, le nombre de failles ou de brèches des nouvelles applications et systèmes d'exploitation augmente également à grande vitesse. L'évolution des menaces informatiques suit donc l'évolution de l'informatique elle-même et celle des

technologies en général. Le constat est donc que les problèmes de sécurité informatiques sont multiformes et multidimensionnels (humains, juridiques, techniques etc.) et face à cette complexité, il existe de multiples solutions parmi lesquels nous avons cité le chiffrement, les pare-feux, les systèmes de protection contre les intrusions etc.

Le problème qui ressort est donc de savoir comment mettre en œuvre ces solutions de manière à pouvoir répondre efficacement et par conséquent de pouvoir réellement bien se protéger de ces menaces multiples et complexes.

Dans ce contexte, la solution que proposent les experts en sécurité est la définition et la mise en application d'une stratégie de sécurité qui se traduit par une politique de sécurité.

Les responsables de sécurité ont donc le devoir de faire tout leur possible pour garantir au mieux la sécurité dans leurs organismes respectifs en mettant en place des stratégies de sécurité adéquates. C'est-à-dire des stratégies de sécurité qui conviennent le mieux aux priorités de leurs organismes. C'est pourquoi, nous allons dans la deuxième partie de notre document voir ce qu'est réellement une stratégie de sécurité.

Chapitre 2 : Les stratégies de sécurité des systèmes d'information

Les principales préoccupations des acteurs de la sécurité sont relatives à l'appréhension globale de la maitrise des risques technologiques et informationnels via une approche intégrative et évolutive, tenant compte des facteurs d'ordre humain, technologique, économique et politique des questions de sécurité.

Entre besoins et solutions de sécurité, entre facilité d'utilisation et efficacité des solutions de sécurité, entre délais de disponibilité de solutions efficaces et coûts de développement et d'intégration, entre niveau de sécurité et coûts des solutions, l'équilibre à trouver passe par un compromis. Ce dernier, résultat émanant du choix consistant à privilégier un facteur au détriment d'autres. Un équilibre est à obtenir entre les besoins de sécurité et les dimensions financières et humaines de la mise en œuvre opérationnelle des solutions de sécurité viables. Le niveau de sécurité des infrastructures résulte donc d'un compromis entre trois principaux facteurs : le coût, le niveau de sécurité et le temps de livraison. Il est illusoire de croire que ces trois facteurs pourraient être satisfaisants simultanément. Des choix doivent être effectués pour déterminer le facteur à favoriser et à partir duquel, les deux autres devront être adaptés.

La sécurité informatique d'une organisation doit s'appréhender d'une manière globale. Elle passe par la définition d'une stratégie de sécurité qui se traduit par une politique de sécurité. Cette dernière comportera la motivation et la formation du personnel, la mise en place de mesures ainsi que par l'optimisation des solutions. L'utilisation d'outils ou de technologies de sécurité ne peut pas résoudre les problèmes de sécurité d'une organisation. En aucun cas, elle ne se substitue à une gestion cohérente de l'ensemble des problèmes de sécurité.

L'abandon des politiques de sécurité « alibi » qu'on rédige juste pour se donner bonne conscience, et l'évolution vers des pratiques concrètes réellement élaborées dans les processus de gestion de l'information, voila donc le défit des années futures.

II.1 Définitions et concepts des stratégies de sécurité

II.1.1 Définitions

L'objet de la sécurité peut se définir comme une contribution à la préservation des forces, des moyens organisationnels, humains, financiers, technologiques et informationnels, dont s'est dotée une organisation pour la réalisation de ses objectifs. La finalité de la sécurité informatique au sein d'une organisation est de garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'entreprise. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et à autoriser le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre.

Une stratégie de sécurité consiste donc à concevoir une conduite générale de protection, d'organisation de la défense (démarche proactive) et d'élaboration de plans de réaction (démarche réactive). Elle s'inscrit dans une approche d'intelligence économique afin de permettre une véritable maîtrise des risques opérationnels, technologiques et informationnels.

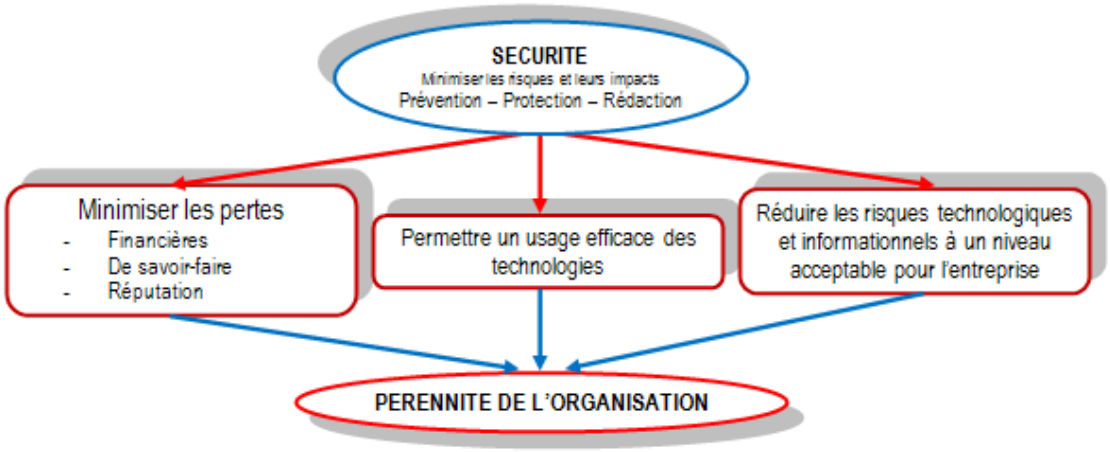


Figure 2-1 : Objectifs de la sécurité

Un risque est un danger éventuel plus ou moins prévisible. Il se mesure à la probabilité qu'il se produise et aux impacts et dommages consécutifs à sa réalisation. Un risque exprime la probabilité qu'une valeur soit perdue en fonction d'une vulnérabilité liée à une menace, à un danger.

La maîtrise des risques informatiques consiste à les réduire à un niveau acceptable pour l'organisation afin d'éviter de mettre en cause sa productivité et sa pérennité.

La frontière entre le risque acceptable et celui qui ne l'est pas est parfois difficile à déterminer objectivement car, elle dépend fortement des objectifs de l'organisation et du degré de criticité de ses ressources.

II.1.2 Concepts des stratégies de sécurité

La mise en place d'une stratégie de sécurité repose sur des invariants qui, s'ils sont adoptés par l'ensemble de l'organisation, facilitent la mise en place et la gestion de la sécurité. Il s'agit des principes de base suivants :

- Principe de vocabulaire qui est une absolue nécessité de s'accorder, au niveau de l'organisation, sur un langage commun de définition de la sécurité ;
- Principe de cohérence, car une accumulation d'outils sécuritaires n'est pas suffisante pour réaliser un niveau global et cohérent de sécurité. La sécurité d'un système d'information résulte de l'intégration harmonieuse des outils, mécanismes et procédures liés à la prévention, à la détection, à la protection et à la correction des sinistres relatifs à des fautes, à la malveillance ou à des éléments naturels ;
- Principe de volonté directoriale qui résulte directement de la considération de l'information comme ressource stratégique de l'entreprise. Il est donc de la responsabilité de ses dirigeants de libérer les moyens nécessaires à la mise en œuvre et à la gestion de la sécurité informatique ;
- Principe financier : le coût de la sécurité doit être en rapport avec les risques encourus. Le budget consacré à la sécurité doit être cohérent vis-à-vis des objectifs de sécurité fixés ;

- Principe de simplicité et d'universalité : les mesures de sécurité doivent être simples, souples, compréhensibles pour tous les utilisateurs et doivent s'appliquer à l'ensemble du personnel ;
- Principe de dynamicité : la sécurité doit être dynamique pour intégrer la dimension temporelle de la vie des systèmes et de l'évolution des besoins et des risques ;
- Principe de continuum : L'organisation doit continuer à fonctionner même après la survenue d'un sinistre. Pour cela, il faut disposer de procédures d'urgence et de reprise ;
- Principe d'évaluation, de contrôle et d'adaptation : il est impératif de pouvoir évaluer constamment l'adéquation des mesures de sécurité au regard des besoins effectifs de la sécurité. Cela permet de contrôler et de vérifier que les risques sont maitrisés de manière optimale dans un environnement dynamique et d'adapter si nécessaire les solutions de sécurité mis en œuvre. Des outils de type « tableau de bord » de la sécurité favorisent le suivi de la sécurité par une meilleure appréciation de la variabilité des critères de sécurité. L'adéquation du niveau de sécurité par rapport aux besoins de sécurité de l'entreprise, qui sont par nature évolutifs, est un souci constant du responsable sécurité.

Une organisation peut ainsi renoncer à mettre en œuvre un dispositif de secours *(backup) de* son centre informatique au regard de son coût récurent. En effet, ce coût peut s'avérer être très élevé en termes de ressources et de procédures à utiliser si l'on tient compte :

- De la probabilité du risque de destruction physique totale des infrastructures ;
- Coût des mesures :
  1. De surveillance et de détection (incendie, inondation, intrusion, etc.) ;
  2. De partitionnement des salles machines ignifugées à deux heures garanties, sur lesquelles sont réparties les applications critiques.

De ce fait, les risques résiduels (attentats, chutes d'avion, etc.) est le plus souvent jugé comme acceptable par les organes dirigeants des institutions.

II.1.2.1 Pourquoi les stratégies de sécurité ?

Les risques et menaces pesant constamment sur les systèmes d'information, une défaillance de la sécurité de ces dernières serait capable d'entrainer des conséquences irréversibles sur la réalisation des objectifs stratégiques de l'organisation ou vis-à-vis de ses collaborateurs ou engagements.

C'est pour cette raison que la stratégie de sécurité doit impérativement provenir des plus hautes sphères dirigeantes de l'organisme, en tant qu'instrument de gestion des risques sécurité du système d'information. La stratégie de sécurité des systèmes d'information traduit fortement la reconnaissance formelle de l'importance accordée par la direction de l'organisme à la sécurité de son ou ses systèmes d'information.

Face à ces menaces sur les systèmes d'information, les utilisateurs exigent une protection adaptée des informations et des services de traitement, d'archivage et de transport de l'information. La sécurité est immédiatement devenue l'une des dimensions essentielles de la stratégie de l'organisme et elle doit être prise en compte dès la conception d'un système

d'information afin d'assurer la protection des biens, des personnes et du patrimoine de l'organisme.

Ainsi, la sécurité des systèmes d'information vise en particulier à protéger les composantes suivantes du patrimoine :

- Le patrimoine matériel, composé de biens matériels nécessaires au fonctionnement de ses activités et dont la détérioration pourrait interrompre, diminuer, ou altérer son activité ; ce patrimoine est essentiellement composé des technologies de l'information et de communication (serveurs, réseaux, postes de travail, téléphonie), mais aussi des procédures et applications logicielles traduisant les processus et les fonctions métiers de l'organisme ;
- Le patrimoine immatériel et intellectuel, composé de toutes les informations concourant au métier de l'organisme (données scientifiques, techniques, administratives) ;
- Les informations relatives aux personnes (physiques ou morales) avec qui l'organisme est en relation, dont la destruction, l'altération, l'indisponibilité ou la divulgation pourrait entrainer des pertes ou porter atteinte à son image de marque voire entrainer des poursuites judiciaires.

II.1.2.2 Conditions de succès d'une démarche sécuritaire

Les conditions de succès de la réalisation d'une stratégie sécuritaire sont, entre autres :

- Une volonté directoriale, car il ne peut y avoir de succès d'une stratégie sans la volonté directoriale ;
- Une politique de sécurité simple, précise, compréhensible et applicable ;
- La publication et diffusion de la politique de sécurité ;
- Une gestion centralisée de la sécurité et une certaine automatisation des processus de sécurité ;
- Un niveau de confiance déterminé des personnes, des systèmes, des outils impliqués ;
- Du personnel sensibilisé et formé à la sécurité, possédant une haute valeur morale ;
- Des procédures d'enregistrement, de surveillance et d'audit assurant la traçabilité des événements pour servir de preuve en cas de nécessité ;
- La volonté d'éviter de mettre les systèmes et les données en situation dangereuse ;
- L'expression, le contrôle et le respect des clauses de sécurité dans les différents contrats ;
- Une certaine éthique des acteurs et le respect des contraintes légales.

L'efficacité des mesures de sécurité d'un système d'information ne repose pas uniquement sur les outils de sécurité, ni sur le budget investi, mais sur la qualité de la stratégie définie, sur l'organisation mise en place pour la réaliser, l'évaluer, la faire évoluer en fonction des besoins. Cela nécessite une structure de gestion adéquate pour concevoir la stratégie, définir une politique de sécurité, gérer, spécifier des procédures et des mesures cohérentes, mettre en place, valider et contrôler.

Il est clair que la stratégie relève du domaine de la direction générale ; il faut donc comprendre que les prérogatives de la structure organisationnelle s'inscrivent dans un degré de délégation appropriée. Cette structure détermine le comportement, les privilèges et les responsabilités de chacun. Elle contribue à faire comprendre à l'ensemble des acteurs de l'organisation l'importance de la sécurité et du respect des règles de sécurité. Elle spécifie (en

fonction de facteurs critiques de succès qui permettent d'atteindre les objectifs de l'entreprise) les mesures et les directives sécuritaires appropriées. Ces dernières doivent être relationnelles par rapport aux plans de l'entreprise et de l'informatique. Une vision stratégique de la sécurité globale de l'organisation est donc primordiale.

II.2 Mise en place d'une démarche sécuritaire

La stratégie de sécurité réside dans un compromis judicieux entre le coût des outils et des procédures à supporter pour pallier les risques réels qui pourraient affecter le patrimoine de l'entreprise et le coût des impacts de la réalisation des risques.

Il n'existe pas de stratégie prédéterminée ou générale, ni de recette pour définir une stratégie. Chaque contexte d'organisation, de scénario de risques ou d'environnement est particulier. On ne peut définir de règles générales qui déterminent quelles sont les stratégies ou solutions de sécurité à implanter pour maîtriser un risque donné.

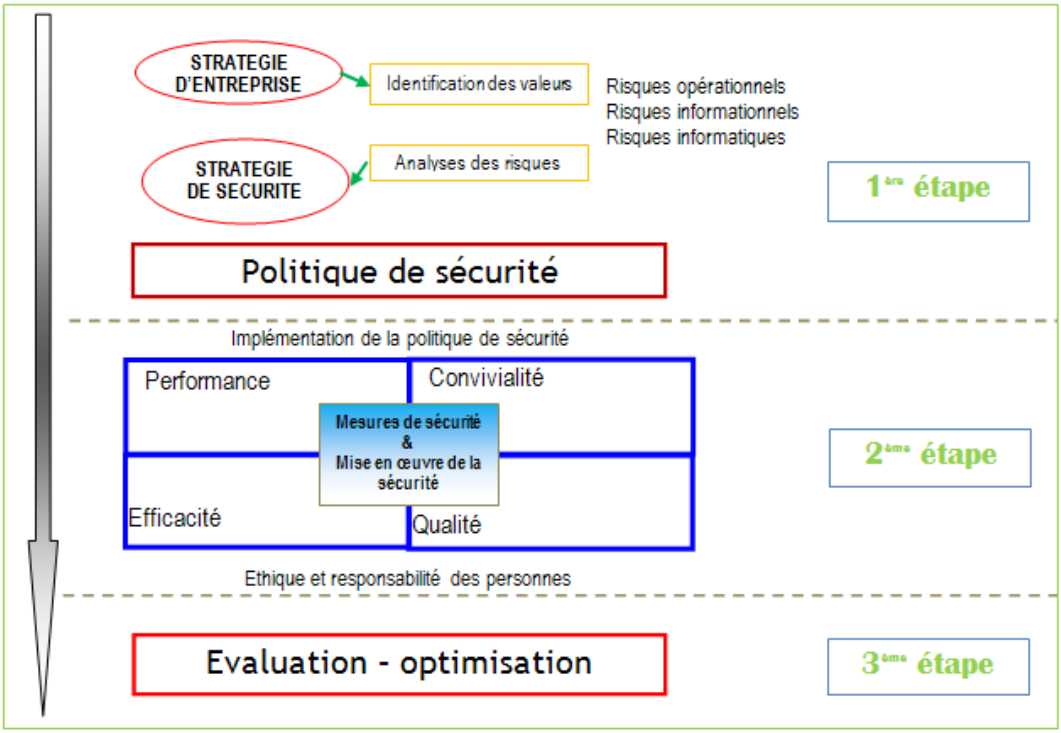


Figure 2-2 : étapes de réalisation d'une démarche sécuritaire

La démarche sécuritaire se subdivise en trois grands axes :

- La stratégie globale d'entreprise ;
- La stratégie de sécurité ;
- La politique de sécurité.

La première étape stratégique consiste à identifier les valeurs de l'entreprise, leur niveau de vulnérabilité en fonction de menaces particulières et le risque de perte totale ou partielle de ces valeurs. À l'issue de cette analyse des risques, une vision de ce qui doit être protégé, contre qui et pourquoi est formulée sous la forme d'une politique de sécurité. Il s'agit alors de définir une véritable stratégie de protection et de gestion de la sécurité en fonction des besoins, valeurs et menaces réelles qu'encoure l'organisation. De la pertinence de l'analyse des

risques dépendra l'identification correcte des moyens et des mesures de sécurité à mettre en œuvre pour protéger efficacement les ressources du système d'information.

L'étape suivante consiste à choisir puis à mettre en place les outils et les procédures nécessaires à la gestion des risques et à la sécurité des systèmes, services et données.

Enfin, il est impératif de contrôler non seulement l'adéquation des solutions de sécurité et leur cohérence les unes par rapport aux autres, mais également la pertinence de la politique de sécurité en fonction des risques et des moyens financiers et la cohérence des outils vis-à-vis de la politique. Une évaluation périodique, voire constante des mesures de sécurité en vue de leur optimisation, permet de répondre au mieux à l'évolution de l'environnement dans lequel elles s'inscrivent.

II.2.1 Méthodes et normes d'élaboration de démarches sécuritaires

II.2.1.1 Principales méthodes françaises

La démarche sécuritaire traite de l'organisation de la sécurité, de l'inventaire des risques relatifs aux actifs informationnels, de la définition d'une architecture de sécurité, de l'établissement d'un plan de continuité.

Pour débuter une démarche sécuritaire, on s'appuie sur une méthode qui facilite l'identification des points principaux à sécuriser (notion de Check List). Dans un premier temps, il faut pouvoir identifier les risques afin d'identifier les parades à mettre en place et gérer le risque résiduel. Jusqu'à présent, la sécurité repose plus sur un ensemble reconnu de bonnes pratiques que sur une méthodologie unique.

Diverses méthodes propriétaires comme des normes internationales existent et peuvent servir de guide à l'élaboration d'une politique de sécurité. Elles sont utilisées plus ou moins complètement et le plus souvent adaptées à un contexte d'analyse.

Les méthodes préconisées par le Clusif (Club de la Sécurité de l'Information Français) sont le MARION (Méthode d'Analyse des Risques Informatiques et Optimisation par Niveau) et MEHARI (Méthode Harmonisée d'Analyse des Risques).

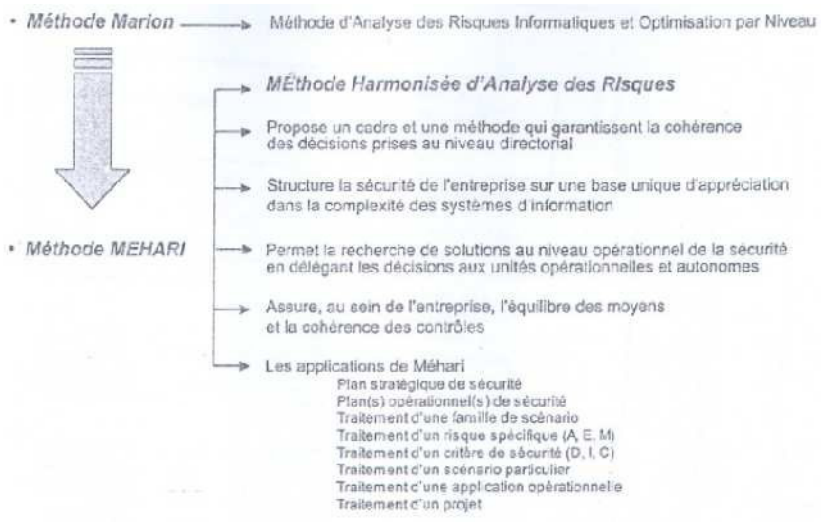


Figure 2-3 : les méthodes préconisées par le Clusif

Au-delà de l'aide à l'analyse des vulnérabilités et des risques, Méhari permet d'avoir une vision globale et stratégique de la problématique de la sécurité des entreprises, par la définition d'un plan stratégique de sécurité à partir duquel des plans opérationnels pourront être définis. Les différents niveaux de la sécurité sont ainsi appréhendés. Les vues stratégiques, tactiques et opérationnelles ainsi que les mesures spécifiques à leurs réalisations sont distinguées.

La méthode d'analyse des risques Méhari se veut adaptable, évolutive et compatible avec la norme ISO 17799.

Par ailleurs, la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) propose une méthode largement documentée, présentée et téléchargeable sur son site (http://www.ssi.gouv.fr). Dénommée Ebios (Expression des besoins et identification des objectifs de sécurité), cette méthode adoptée par les administrations françaises, permet de spécifier les objectifs de la sécurité des organisations, pour répondre à des besoins déterminés. Elle facilité largement l'appréhension du contexte de sécurité et constitue une véritable aide à la définition des objectifs et des politiques de sécurité. Cela peut conduire à remplir le document « Fiche d'Expression Rationnelle des Objectifs de Sécurité (Feros) » pour ce qui concerne toutes les ressources classées « défense », afin de déterminer au mieux les mesures de sécurité nécessaires à leur protection.

Il existe également diverses directives nationales : allemandes issu du Bundesamt für Sicherheit Informationstechnik, canadiennes du CST (Centre de la Sécurité des Télécommunications), américaines issues du NSI (National Standards Institue) des Etats-Unis, par exemple, qui traitent des politiques de sécurité.

II.2.1.2 Normes internationales ISO/IEC 17799

L'origine de la norme ISO 17799 adoptée par l'ISO à la fin de l'année 2000 est la norme BS 7799 élaborée par l'association de normalisation britannique en 1995. Avant d'être reconnue comme une méthode de référence, la norme internationale ISO 17799 a tout d'abord été contestée du fait de sa procédure accélérée de normalisation : elle n'avait pas été révisée par les états membres avant d'être publiée et n'avait donc pas tenu compte des savoir-faire et autres méthodes existants dans d'autres pays.

L'adoption par le marché de la norme ISO a été favorisée par le fait que certaines compagnies d'assurance demandent l'application de cette norme afin de couvrir les cyber-risques.

Basée sur la gestion des risques, la norme propose un code de pratique pour la gestion de la sécurité et identifie des exigences de sécurité sans toutefois spécifier la manière de les réaliser. On peut ainsi considérer cette norme tour à tour comme un référentiel contribuant à la définition d'une politique de sécurité, comme une liste de points de risques à analyser (Check List), comme une aide à l'audit de sécurité en vue ou non d'une procédure de certification ou encore, comme un point de communication sur la sécurité. Diverses interprétations et réalisations de cette norme sont possibles.

Son intérêt réside dans le fait que la norme aborde les aspects organisationnels, humains, juridiques et technologiques de la sécurité en rapport aux différentes étapes de conception, mise en œuvre et maintien de la sécurité.

1. Politique de sécurité
2. Organisation de la sécurité
3. Classification et contrôle des actifs
4. Sécurité et gestion des ressources humaines
5. Sécurité physique et environnementale
6. Exploitation et gestion de systèmes et de réseaux
7. Contrôle d'accès
8. Développement et maintenance des systèmes
9. Continuité des services
10. Conformité

Figure 2-4 : Domaines de sécurité de la norme ISO 17799 2000.

Elle traite de dix domaines de sécurité, de 36 objectifs de sécurité et de 127 points de contrôle. Une nouvelle version de cette norme (lSO/IEC 17799 : 2005) a été éditée en juillet 2005, elle adjoint aux dix domaines de sécurité préalablement identifiés de nouveaux paragraphes qui concernent l'évaluation et l'analyse des risques, la gestion des valeurs et des biens ainsi que la gestion des incidents. On remarque toute l'importance accordée à la dimension managériale de la sécurité dans la nouvelle version.

II.2.2 La stratégie globale d'entreprise

En raison du caractère évolutif du contexte (évolution des besoins, des risques, des technologies, des savoir-faire des cyber-délinquants), les solutions de sécurité ne sont jamais ni absolues, ni définitives. Cela pose le problème de la pérennité des solutions mises en place. De plus, la diversité et le nombre de solutions peuvent créer un problème de cohérence globale de l'approche sécuritaire. En conséquence, la technologie ne suffit pas, elle doit être intégrée dans une démarche de gestion.

Ainsi, la technologie sécuritaire doit être au service d'une vision politique de la sécurité. Seule la dimension managériale de la sécurité permet de faire face au caractère dynamique du risque. C'est la qualité de la gestion qui permet de tirer le meilleur parti des outils existant et qui apporte une réelle plus-value au service de la sécurité. Dans cette perspective, la sécurité du système d'information n'est qu'une composante de la sécurité globale de l'organisation. Il est donc extrêmement important que les orientations stratégiques en matière de sécurité soient déterminées au niveau de l'état-major de la structure concernée.

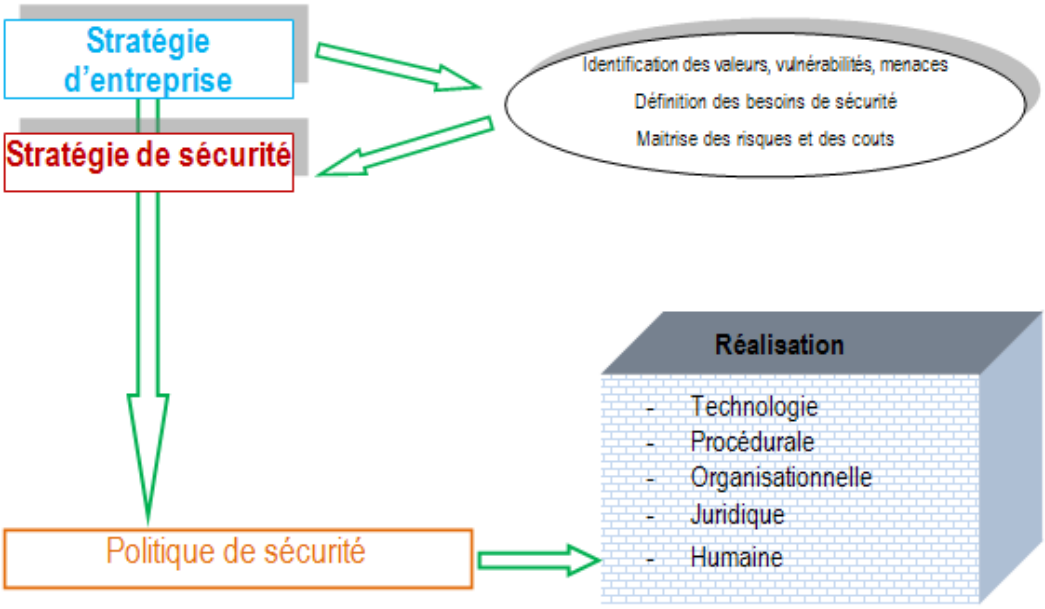


Figure 2-5 : De la stratégie d'entreprise à la stratégie sécuritaire

La stratégie globale d'entreprise est élaborée par la ligne managériale au plus haut niveau de l'organisation. Son objectif est de dégager les objectifs de sécurité de l'organisation pour faire en sorte que toutes les actions entreprises et mises en place dans toutes les composantes de l'organisation (partenaires, sites distants, clients, télétravailleurs) concourent vers les mêmes objectifs et protègent les ressources en fonction de leur criticité).

Une politique de sécurité offre une réponse graduée à un problème sécuritaire spécifique, en fonction de l'analyse des risques qui en est faite. Elle doit exprimer l'équilibre entre les besoins de production et de protection.

Le choix des mesures de sécurité résulte généralement d'un compromis entre le coût du risque et celui de sa réduction. Il dérive de l'analyse à long, moyen et court terme des besoins de production et de protection.

Figure 2-6 : la sécurité, un compromis

La définition d'une stratégie de sécurité est une affaire de bon sens, de vision, d'analyse et de choix. Elle pourrait se résumer à une suite de questions simples auxquelles le gestionnaire doit apporter des réponses précises :

- Quelles sont les valeurs de l'organisation ?
- Quel est leur niveau de sensibilité ou de criticité ?

- De qui, de quoi doit-on se protéger ?
- Quels sont les risques encourus ?
- Ces risques sont-ils supportables ?
- Quel est le niveau actuel de sécurité ?
- Quel est le niveau de sécurité que l'on désire atteindre ?
- Comment passer du niveau actuel au niveau désiré ?
- Quelles sont les contraintes effectives ?
- Quels sont les moyens disponibles ?

Ce sont là tous les défis qui guettent les organisations qui se décident à mettre en œuvre une démarche sécuritaire.

II.2.3 Les stratégies de sécurité des systèmes d'information

Réduire la sécurité à sa dimension technologique c'est assurer son échec. Par ailleurs, se retrancher derrières des règles de sécurité prédéterminées, des réglementations ou des produits « leaders » du marché dans leur niche sécuritaire sans valider leur adéquation aux besoins de l'organisation, mais uniquement par soucis de ne pas engager sa responsabilité, met en péril la mission de sécurité.

Le fossé est souvent assez étroit entre la stratégie d'entreprise et la stratégie de sécurité d'une organisation ; elles concourent toutes les deux à la mise en place de la politique de sécurité et serviront plus tard de document de référence pour évaluer l'efficacité de la politique mise en place.

Chaque organisation doit spécifier sa propre mission de sécurité pour réaliser sa stratégie de sécurité telle que définie avec la direction générale. L'activité de cette mission peut se décliner selon les axes suivants :

- L'identification des valeurs et classification des ressources de l'organisation ;
- La conception d'un plan de sécurité en fonction d'une analyse préalable des risques ;
- La définition d'un périmètre de vulnérabilité lié à l'usage des nouvelles technologies ;
- L'identification des impacts.

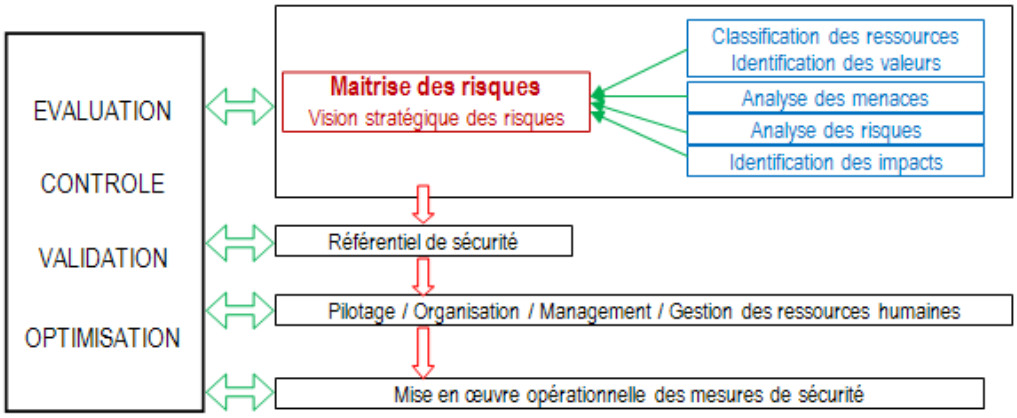


Figure 2-7 : Maitrise des risques et processus de sécurité

Seule une approche pragmatique, inscrite dans une démarche qualité qui définit précisément des objectifs de sécurité cohérents ainsi que des moyens concrets pour les atteindre, permet de sécuriser rationnellement des ressources informatiques partagées.

II.2.3.1 Identification des valeurs et classification des ressources

Le Club de la Sécurité de l'Information Français (CLUSIF), dans son rapport d'enquête sur la sécurité des systèmes d'information confirme qu'en 2008 encore, l'informatique est perçue comme stratégique par une très large majorité des entreprises : tous secteurs confondus et quelque soit leur taille, 73% d'entre elles jugent lourde de conséquences une indisponibilité de moins de 24h de leurs outils informatiques (avec un maximum de 83% pour le secteur du commerce).

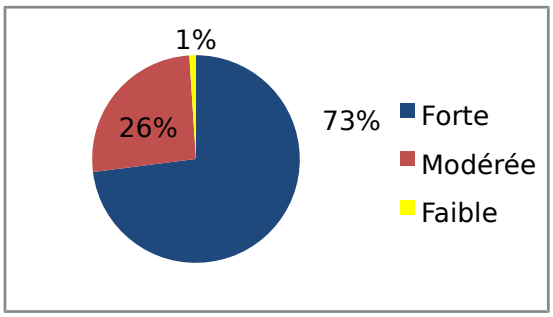


Figure 2-8 : Niveau d'importance de l'informatique dans les entreprisses françaises en 2008

La réalisation d'un inventaire complet et précis de tous les acteurs et intervenants de la chaine sécuritaire contribue à une meilleure connaissance et donc à la maitrise de l'environnement à protéger. C'est dans les phases d'analyse de l'existant et des risques que ces données d'inventaire prennent toute leur importance. Elles interviennent également dans la phase d'identification des valeurs et de classification des ressources pour déterminer leur degré de sensibilité ou de criticité. Le degré de criticité d'une ressource indique son importance en cas de perte, d'altération ou de divulgation des données. Plus les conséquences sont graves pour l'organisation, plus la ressource est sensible et possède de la valeur. La classification selon le degré d'importance des ressources à protéger, est nécessaire à la gestion de la sécurité. Elle est dispensable à l'élaboration future de la politique de sécurité pour définir des mesures et procédures à appliquer.

Chaque ressource peut être perçue comme une cible de sécurité pour laquelle, il faut identifier les risques et leurs scénarii possibles (erreur d'utilisation ou de paramétrage, accidents, malveillance, sabotage, attaque logique, etc.), les mécanismes de sécurité inhérents et applicatifs (configuration, paramètres, etc.), ainsi que les contraintes techniques et organisationnelles afin de déterminer la faisabilité technique et organisationnelle de la politique de sécurité pour chaque cible.

La détermination du degré de sensibilité des données consiste tout d'abord à identifier des classes génériques de données auxquelles on associe des valeurs entières définissant leur degré de sensibilité. Cela permet de disposer d'une métrique, dont l'échelle des valeurs est déterminée par l'organisation et qui reflète le degré d'importance de la donnée pour celle-ci. Ainsi, par exemple, pour une entreprise les données peuvent être classées :

- Publiques : degré de sensibilité 0 ; 1 ;
- Financières : degré de sensibilité 1 ;
- Privées : degré de sensibilité 2 ;

- Secrètes : degré de sensibilité 3 ;

Cette classification doit être affinée voire adaptée en fonction des besoins. De plus, c'est en fonction du degré de sensibilité des données et du profil des utilisateurs que l'on attribuera à ces derniers, des permissions et droits d'accès.

L'identification des valeurs du système d'information d'une organisation répond essentiellement à la question : « Quelles informations sont critiques pour les besoins opérationnels de l'organisation ? ». Ceci permettra de dresser un inventaire de toutes les ressources ou processus qui entrent dans le fonctionnement normal de l'organisation.

Cette étape peut se révéler assez complexe dans le cadre d'un système d'information peu ou pas modélisé, ne répondant généralement à aucun standard ; avec des processus métiers non élaborés. Elle constituera aussi une sorte de début d'audit pour le système d'information ; et donnera un aperçu du niveau de complexité des processus. Il est clair qu'un système d'information qui a du mal à révéler ses valeurs sera très difficile à sécuriser ; puisque les brèches de sécurité seront nombreuses et subtiles.

A l'issue de cette étape d'inventaire des ressources, une classification du niveau de criticité des informations, des processus, des systèmes et des réseaux constituera l'épreuve de la mission de sécurité.

II.2.3.2 Analyse des risques

Un risque provient du fait qu'une organisation ou une entité possède des « valeurs » matérielles ou immatérielles qui sont susceptibles de subir des dommages ou une dégradation. Cette dernière ayant des conséquences pour l'organisation concernée : ceci fait généralement appel à quatre notions :

- Celle de la « valeur », qu'il est d'usage d'appeler « actif » dans le domaine de la sécurité des systèmes d'information ;
- Celle de dégradation ou de dommage subi par l'actif ;
- Celle de conséquence pour l'entité ;
- Celle qui suggère une cause possible mais non certaine ;

CONFIDENTIALITE	DISPONIBILITE	INTEGRITE
Perte de confidentialité sans conséquence	**Délai supérieur à une semaine**	**Perte d'intégrité sans conséquence**
Le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités de l'organisme. Ex : données publiques, visibles par tous.	Des services qui apportent un confort supplémentaire mais pas indispensable.	Le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités de l'organisme. Ex : aucune vérification.
Perte de confidentialité entraînant des gênes de fonctionnement	**Délai > 8 heures et <= 1 semaine**	**Perte d'intégrité entraînant des gênes de fonctionnement**
Susceptible de provoquer une diminution des capacités de l'organisme. Ex : données liées aux compétences ou savoir-faire internes, dans un contexte de groupe de confiance, dont vous protégez toutes les traces écrites.	Ressources pour lesquelles il existe une alternative. Ex : imprimantes.	Susceptible de provoquer une diminution des capacités de l'organisme. Ex : vérification des données, sans validation : des fautes d'orthographe sur une page web nuisent à l'image de marque du laboratoire.
Perte de confidentialité entraînant des conséquences dommageables	**Délai > 2heures et <= 8 heures**	**Perte d'intégrité entraînant des conséquences dommageables**
Susceptible d'amoindrir les capacités de l'organisme, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation Ex : données liées à un engagement de confidentialité dans un contrat.	Sans conséquence vitale humainement Ex : arrêt du réseau, de la messagerie, données vitales non disponibles...	Susceptible d'amoindrir les capacités de l'organisme, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation Ex : données qui sont validées et contrôlées par des moyens techniques ou humains.
Perte de confidentialité entraînant des conséquences graves	**Délai : entre temps réel et <= 2 heures**	**Perte d'intégrité entraînant des conséquences graves**

Susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières. Ex : données secret défense.	Ressources qui mettent en péril la vie (humaine ou animale ou biologique). Ex : expériences biologiques ou physiques pilotées automatiquement, système de sécurité.	Susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières. Ex : données avec au moins deux niveaux de validation et de contrôle différents (techniques ou humains)

Tableau 2-1 : Analyse des risques des systèmes d'information

II.2.4 Les politiques de sécurité

Depuis le début des années 2000, la prise en compte par les organisations des problèmes liés à la sécurité informatique s'est généralisée au moins dans les grandes structures. La sécurité est de moins en moins une juxtaposition de technologies hétérogènes de sécurité. Elle est dorénavant appréhendée et traitée, comme un processus continu. Cette vision « processus » met en avant la dimension managériale de la sécurité qui vise à l'optimisation et la rationalisation des investissements, tout en assurant la pérennité et l'efficacité des solutions de sécurité dans le temps.

Politique de sécurité				
Politique de contrôle d'accès	Gestion des identités, des profils des utilisateurs, des permissions, des droits, etc.	Mesures et procédures	Convivialité Coût Performance	Respect des contraintes légales et réglementaires
Politique de protection	Prévention des intrusions et malveillances, Gestion des vulnérabilités, dissuasion, etc.			
Politique de réaction	Gestion des crises, des sinistres, des plans de continuité, de reprise, de modification, d'intervention, de poursuite, etc.			
Politique de suivi	Audit, évaluation, optimisation, contrôle, surveillance, etc.			
Politique d'assurance	Politique de sensibilisation			

Tableau 2-2 : Les différentes composantes d'une politique de sécurité

L'importance d'une gestion rigoureuse de la sécurité des systèmes d'information, et de son appréhension globale et intégrée dans les cycles de décision de l'entreprise, est reflétée par l'adoption par les organisations de la notion de gouvernance de la sécurité. Cette dernière traduit la volonté de diriger, de conduire, d'influencer de manière déterminante la sécurité, voire de dominer les risques liés à l'insécurité technologique. Elle possède également une connotation de pouvoir politique qui positionne le problème de la sécurité au niveau stratégique et opérationnel. L'apparition de nouvelles fonctions, comme celles de responsabilité sécurité, intégrées ou non à la direction générale, à la direction des systèmes d'information, ou encore au sein d'une direction métier ou audit, concrétise cette notion liée à la gouvernance de la sécurité.

Compte tenu de la nouvelle importance accordée à la sécurité et à la manière stratégique et globale de l'appréhender, une politique de sécurité, devient l'expression de la stratégie sécuritaire des organisations. Elle constitue pour les organisations, un outil indispensable non

seulement à la gouvernance de la sécurité mais aussi à la réalisation du plan stratégique de sécurité.

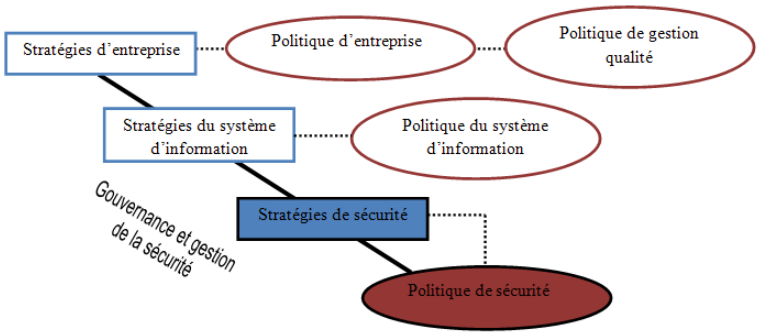


Figure 2-9 : Stratégies et politiques de sécurité

Une politique de sécurité exprime la volonté managériale de protéger les valeurs informationnelles et les ressources technologiques de l'organisation. Elle spécifie les moyens (ressources, procédures, outils, etc.) qui répondent de façon complète et cohérente aux objectifs stratégiques de sécurité.

Elle découle des grands principes de sécurité qui permettent de protéger le système d'information en évitant qu'il ne devienne une cible et en faisant en sorte qu'il ne se transforme pas lui-même en acteurs d'attaques par une prise de contrôle à distance (les Botnets).

Cette protection est assurée par exemple par :

- Des règles : classification de l'information ;
- Des outils : chiffrement, des firewalls ;
- Des contrats : clauses et obligations ;
- L'enregistrement, la preuve, l'authentification, l'identification, le marquage ou le tatouage ;
- Le dépôt des marques, de brevets, et la protection du droit d'auteur.

En complément, elle pourra prévoir de :

- Dissuader par des règles et des contrôles ;
- Réagir par l'existence de plans de secours, de continuité et de reprise ;
- Gérer des incidents majeurs par un plan de gestion de crise ;
- Poursuivre en justice et de demander des réparations en prévoyant un plan d'intervention et de report des incidents et des mesures d'assurance, par exemple ;
- Gérer les performances et les attentes des utilisateurs.

II.3 Cas pratiques d'une démarche sécuritaire au sein d'une PME

L'objectif de ce cas pratique est de montrer les étapes à suivre pour mener dans de bonnes conditions une démarche sécuritaire. Il s'appuie sur la méthode MEHARI 2007 du Clusif, mais apporte des améliorations et des simplifications pour un réajustement de ce standard français aux réalités de nos entreprises locales qui ont souvent des systèmes d'informations

peu ou pas du tout modélisés ; avec des processus très mal élaborés et souvent sans aucune charte d'utilisation.

II.3.1 Présentation de la PME

II.3.1.1 Présentation générale

« Bénin Cosmetics » est une société fictive inventée pour servir de cadre d'expérimentation à notre étude. Nous lui avons fait hériter de toutes les caractéristiques des PME locales. Elle est spécialisée dans la fabrication et la distribution de produits cosmétiques ; elle a son unité de fabrication à Parakou (environ 400 Km au nord de Cotonou), et son siège social à Cotonou. Son effectif total s'élève à environ 250 personnes.

« Bénin Cosmetics » conçoit de nouvelles gammes de produits de beauté et de procédés chimiques de fabrication au siège social pour l'usine de Parakou. Sa puissante équipe de recherche constituée de chimistes, d'esthéticiens, de dermatologues et de biologistes lui a permis de se faire très rapidement une solide réputation dans la sous-région en terme d'innovations dans la fabrication de produits de beauté. Pour cela, elle s'appuie sur son système d'informations qui lui permet d'être vif aux demandes des clients et les nouvelles possibilités de partenariat.

II.3.1.2 Patrimoine informatique

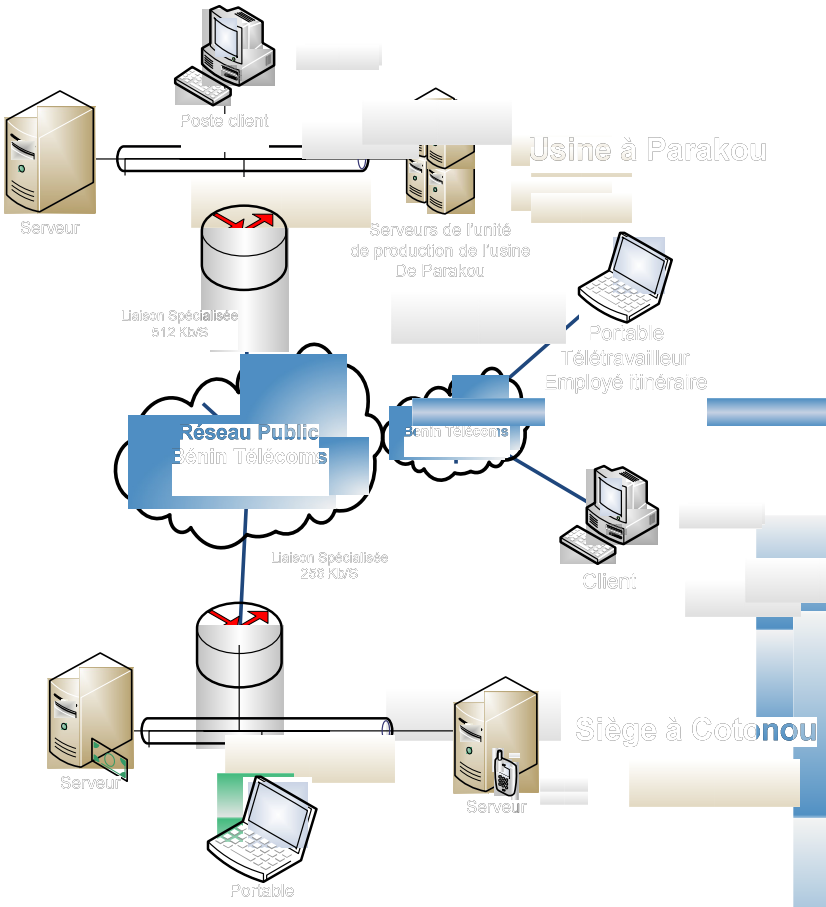


Figure 2-10 : Schéma synthétique du système d'information de « Bénin Cosmetics »

1. Matériel

Le patrimoine du système d'information est constitué d'équipements hétérogènes :

- Des serveurs pour le stockage, le traitement et le partage de l'information ;
- Des ordinateurs de bureau qui sont de type PC ;
- Les réseaux LAN du siège social de Cotonou et l'usine de Parakou sont de type Giga-Ethernet ;
- Les réseaux WAN d'interconnexion et d'accès à Internet sont gérés par l'opérateur historique des télécommunications au Benin « Bénin Télécoms SA », fournisseur de services Internet ;

2. Logiciels

La moitié des systèmes d'exploitation a été légalement acquise et possèdent des numéros de licence valides ;

II.3.1.3 La sécurité

Le système d'information

« Bénin Cosmetics » possède une politique de sécurité du système d'information ; elle fait partie intégrante de la politique globale de sécurité de l'organisation. Une charte d'utilisation des ressources informatiques et des services Internet a été élaborée et diffusée à l'ensemble du personnel. Elle précise les droits et devoirs de chaque utilisateur. La charte peut se résumer en plusieurs points:

- Le contrôle d'accès se fait par authentification avec un nom d'utilisateur et un mot de passe ;
- Obligation de suivre la procédure de sauvegarde pour tous les documents numériques de l'entreprise ;
- La responsabilité de chaque utilisateur sur tous les fichiers qu'il traite, les fichiers sont sauvegardés sur les serveurs ; les documents papiers conservés dans des armoires sécurisées ;
- Chaque utilisateur est directement responsable des ressources informatiques mises à sa disposition dans le cadre de son activité ;
- Chaque utilisateur doit signaler toute anomalie constatée ou comportement bizarre du système dans les plus courts délais au département informatique ;

Sécurité générale du siège social à Cotonou

- Pare-feux, détection et extinction d'incendie des locaux ; des exercices annuels d'évacuation sont réalisés une fois par an en collaboration avec les services de sécurité de l'immeuble ;
- Existence de consigne de fermeture des bureaux à clé, mais aucune procédure de contrôle ;
- Conditionnement de la température de toutes les pièces ;

- Existence de technologies de surveillance (camera de surveillance, alarme anti-intrusion, détecteur de mouvement) activée durant les heures de fermetures (18h45 – 07h15) ; des agents de sécurité veillent sur les lieux ;
- L'entretien des locaux se fait tous les matins de 07h30 à 08h par une société prestataire ;
- L'accès aux bureaux est conditionné par un badge magnétique d'authentification ;
- Les clients sont reçus par les agents commerciaux, dans les salles de réunion dans une zone avec vidéosurveillance ; il y a possibilité de connecter des équipements informatiques ;
- Les ressources informatiques (serveurs, routeurs, autocommutateurs) sont situées dans une salle isolée du département informatique ; elle possède une alimentation électrique de secours ;

Sécurité générale de l'usine à Parakou

- Pare-feux, détection et extinction d'incendie des locaux ; des exercices annuels d'évacuation sont réalisés trois fois par an en collaboration avec les services de sécurité de l'immeuble ;
- Poste de gardiennage qui filtre les entrées et sorties sur le site de l'usine, une gestion technique centralisée pour l'ensemble des alarmes du site avec deux personnes en permanence.
- Consignes de fermeture à clé des bureaux ; mais aucune procédure de contrôle n'a été mise en place ;
- Tous les bureaux sont climatisés ; et contigus au poste de gardiennage ; à l'entrée de l'usine ; à l'écart des zones de production ;
- Alarme anti-intrusion est active durant les heures de fermeture des bureaux (19h- 7h), de fréquentes rondes de gardiens ont lieu dans le bâtiment ;
- Le service de nettoyage externe à l'entreprise intervient de 7h à 8h ;
- Plusieurs sociétés constituent son voisinage ; de fréquentes rondes de police ont lieu dans la zone d'activité ;
- Les clients sont reçus, sous la responsabilité de la personne visitée après avoir déposé une pièce d'identité contre la remise d'un badge visiteur au poste de gardiennage, dans des salles de réunions spécifiques ; avec possibilité de connecter des équipements informatiques ;

Le site possède la redondance pour les fournitures énergétiques (arrivée électrique provenant de 2 cabines "Haute Tension", groupe électrogène, onduleurs, arrivée lignes téléphoniques sur 2 centraux téléphoniques différents, etc.).

II.3.1.4 Contexte

L'interconnexion du siège de Cotonou à l'usine de Parakou a permis d'avoir un système d'information unifié au niveau connectivité. Ce qui a permis une nette amélioration des délais de réalisation des travaux et de faire des gains en coûts de communication ou de liaison.
« Bénin Cosmetics » a répondu au vœu de ses différents partenaires qui est de correspondre directement avec les différents services via Internet pour la transmission de tous types de documents (dossiers techniques, devis, appels d'offres, messages, etc.).

D'autre part, un important contrat de collaboration avec une chaine de cosmétique basée en France est conditionné par la capacité de « Bénin Cosmetics » à assurer :

- La confidentialité dans les échanges des documents techniques (formules chimiques, procédés de fabrication, etc.) ;
- La disponibilité et la rapidité de fournir des produits finis ;

II.3.2 Application de la démarche MEHARI

II.3.2.1 Présentation de la méthode MEHARI

MEHARI signifie « MEthode Harmonisée d'Analyse des RIsques ». Il s'agit d'une méthode élaborée en 1996 par le CLUSIF (Club de la Sécurité de l'Information Français) pour définir les actions en termes de sécurité des Systèmes d'Informations au sein des organisations. Le CLUSIF fournit les différents supports aidant à la mise en place d'une démarche sécuritaire selon la méthode MEHARI.

La démarche Méhari comporte trois grandes phases :

Plan stratégique de sécurité (PSS) :

- Métrique des risques et objectifs de sécurité ;
- Valeurs de l'entreprise : classification des ressources ;
- Politique de sécurité ;
- Charte de management ;

Plan Opérationnel de sécurité (POS) :

- Audit de l'existant ;
- Evaluation des besoins de sécurité ;
- Expression des besoins de sécurité ;
- Construction du plan opérationnel de sécurité ;

Plan Opérationnel d'Entreprise (POE) :

- Choix d'indicateurs représentatifs ;
- Elaboration d'un tableau de bord de la sécurité de l'entreprise ;
- Rééquilibrage et arbitrage entre unités.

II.3.2.2 Le plan stratégique de sécurité

Le plan stratégique de sécurité (PSS) constitue la première phase de la Méthode Harmonisée d'Analyse des Risques (MEHARI). Elle est élaborée en étroite collaboration avec la ligne managériale de l'entreprise de manière à ce que toutes les actions entreprises et mises en place dans l'ensemble de l'entreprise (sites distants et accès distants inclus) tendent vers ces mêmes objectifs et protègent les ressources en fonction de leur classification.

Il sera un indicateur-clé des unités opérationnelles pour ce qui concerne les décisions à prendre en matière de sécurité. Elle verra la participation de la direction générale de l'entreprise, ainsi que celle des cadres supérieurs responsables de chaque département opérationnel.

II.3.2.2.1 Métrique des risques et objectifs de sécurité

L'objectif de la métrique des risques et objectifs de sécurité est de dégager, par des tableaux standards, communs à toute l'entreprise, les éléments permettant :

- D'une part, d'affecter un degré de criticité de chaque scénario de sinistre ;
- D'autre part, de fixer de façon cohérente les objectifs de sécurité en fonction des niveaux préétablis d'acceptation ou de refus, total ou sous condition, des risques encourus.

Statuts de protection	Effet des mesures de protection sur l'impact du scénario
1	Effet de protection très faible : le sinistre ne sera détecté qu'au bout d'un délai important. Les mesures qui pourront alors être prises ne pourront limiter la propagation de l'incident initial et se limiteront à la borner dans le temps. L'étendue des conséquences du sinistre est difficile à cerner.
2	Effet de protection moyen : le début de sinistre ne sera pas identifié très vite et les mesures prises le seront tardivement. Le sinistre aura pris une grande ampleur mais l'étendue de ses conséquences sera encore identifiable.
3	Effet important : le sinistre sera détecté rapidement et des mesures de protection seront prises sans délai. Le sinistre aura néanmoins eu le temps de se propager, mais les dégâts seront circonscrits et facilement identifiables.
4	Effet très important : le début de sinistre sera détecté en temps réel et les mesures déclenchées immédiatement. Le sinistre sera limité aux détériorations directes provoquées par l'accident, l'erreur ou la malveillance.

Tableau 2-3 : Mesures de protection

Statuts palliatifs	Effet des mesures palliatives sur l'impact du scénario
1	Effet très faible : les solutions de secours éventuellement nécessaires doivent être improvisées. Il n'est pas assuré que les activités de l'entreprise touchées par le sinistre pourront être poursuivies. L'activité de l'ensemble des acteurs touchés par le sinistre est très fortement perturbée.
2	Effet moyen : les solutions de secours ont été prévues globalement et pour l'essentiel, mais l'organisation de détail reste à faire. Les activités principales touchées pourront se poursuivre après un temps d'adaptation qui peut être long. La reprise des autres activités et le retour à l'état d'origine demandera des efforts importants et occasionnera une forte perturbation des équipes.
3	Effet important : les solutions de secours ont été prévues, organisées dans le détail et validées. Les activités principales pourront se poursuivre après un temps de reconfiguration acceptable et connu. La reprise des autres activités et le retour à l'état d'origine ont également été prévus et se dérouleront avec des efforts importants mais supportables.
4	Effet très important : le fonctionnement des activités de l'entreprise est assuré sans discontinuité notable. La reprise de l'activité en mode normal est planifiée et sera assurée sans perturbation notable.

Tableau 2-4 : Mesures palliatives

Statuts récupération	Effet des mesures prises sur l'impact du scénario
1	Effet très faible : ce que l'on peut espérer récupérer des assurances ou d'un recours en justice est négligeable devant l'ampleur des dégâts subis.
2	Effet moyen : ce que l'on peut raisonnablement espérer récupérer n'est pas négligeable, mais les sinistres majeurs restent à la charge de l'entreprise (sinistre non couvert et responsable non solvable).
3	Effet important : l'entreprise est couverte pour les sinistres majeurs, mais ce qui reste à sa charge (franchise) demeure important quoique supportable.
4	Effet très important : l'entreprise est suffisamment couverte pour que l'impact financier résiduel soit négligeable.

Tableau 2-5 : Mesures de récupération

Statuts RI	Effet des mesures prises sur la réduction d'impact du scénario
1	Effet très faible
2	Effet moyen : impact maximum jamais supérieur à un impact grave : I<ou = 3
3	Effet important : impact maximum jamais supérieur à un impact moyennement grave : I<ou= 2
4	Effet très important : impact du scénario toujours négligeable quel que soit l'impact intrinsèque

Tableau 2-6 : Mesures de réduction d'impact du scénario

La grille suivante, proposée en standard, permet d'évaluer l'impact "I":

Classification des ressources / Statuts-RI	1	2	3	4
1	1	2	3	4
2	1	2	3	3
3	1	2	2	2
4	1	1	1	1

Tableau 2-7 : Grille d'évaluation de l'impact de scénario

Statuts exposition	Effet des mesures structurelles sur la potentialité du scénario
1	Exposition très faible : Des mesures architecturales ont été prises pour limiter structurellement les risques : cloisonnement des locaux, fragmentation des informations, rendant négligeable la probabilité d'un risque majeur.
2	Exposition faible : L'entreprise (le service ou l'unité) est particulièrement peu exposée : le climat social est très favorable, l'environnement ne laisse pas craindre le moindre problème, la position de suiveur de l'entreprise rend peu probable une agressivité notable de concurrents.
3	Exposition moyenne : L'entreprise (le service ou l'unité) n'est pas particulièrement exposée. Le climat social n'est pas mauvais, la concurrence est normalement agressive sans plus, l'environnement ne présente pas de menace particulière.
4	Exposition importante : L'entreprise (le service ou l'unité) est particulièrement exposée au risque envisagé de par un climat social est très défavorable ou un environnement à risque ou une position telle que l'on peut craindre des réactions spécialement agressives de la concurrence.

Tableau 2-8 : Tableau mesure des effets d'exposition naturelle

Statuts dissuasion	Effet des mesures dissuasives sur la potentialité du scénario
1	Effet très faible : L'auteur n'encourait aucun risque : il n'a pratiquement aucun risque d'être identifié et de toute façon cela n'aurait pour lui aucune conséquence.
2	Effet moyen : L'auteur encourait un risque faible : le risque d'être identifié est faible et les sanctions éventuelles, s'il était découvert, resteraient supportables.
3	Effet important : L'auteur de l'erreur ou de la malveillance encourrait un risque important : il existe une forte probabilité qu'il soit découvert et les sanctions encourues pourraient être graves.
4	Effet très important : Seul un inconscient pourrait courir un tel risque : il sera démasqué à coup sûr, les sanctions seront très lourdes et tout cela est bien connu.

Tableau 2-9 : Mesure dissuasives

Statuts prévention	Effet des mesures préventives sur la potentialité du scénario
1	Effet très faible : Toute personne de l'entreprise ou tout initié la connaissant un minimum est capable de déclencher un tel scénario, avec des moyens qu'il est facile d'acquérir. Des circonstances tout à fait courantes (maladresse, erreur, conditions météo défavorables rares mais n'ayant rien d'exceptionnel) sont à même de déclencher un tel scénario.
2	Effet moyen : Le scénario peut être mis en œuvre par un professionnel sans autres moyens que ceux dont font usage les personnels de la profession. Des circonstances naturelles rares mais non exceptionnelles peuvent aboutir à ce résultat.
3	Effet important : Seul un spécialiste ou une personne dotée de moyens importants décidée à y consacrer du temps peut aboutir dans la réalisation d'un tel scénario. Des concours de circonstances peuvent rendre le scénario plausible.
4	Effet très important : Seuls quelques experts sont capables, avec des moyens très importants, de mettre en œuvre un tel scénario. Au niveau des événements naturels, seules des circonstances exceptionnelles peuvent conduire à de tels résultats (catastrophes naturelles).

Tableau 2-10 : Mesures préventives

Le niveau de la potentialité "P" est apprécié conformément à la grille standard ci-après :

Statuts potentialité	Potentialité
1	Potentialité faible, ne surviendra sans doute jamais
2	Possible, bien que potentialité faible
3	Potentialité certaine, devrait arriver un jour
4	Très forte potentialité, surviendra sûrement à court terme

Tableau 2-11 : Grille du niveau de potentialité

L'élaboration des définitions des objectifs de sécurité doit faire l'objet d'une réflexion approfondie au plus haut sommet de « Benin Cosmetics » puisqu'elle matérialise ses choix stratégiques en matière de sécurité du système d'informations.

Dans la mesure où il serait totalement utopique de prétendre au « zéro-risque » pour un système d'information, la définition des objectifs de sécurité permet de fixer les niveaux de risque que l'entreprise jugera acceptables, inadmissibles quoique supportables, ou insupportables parce que ne disposant pas des moyens pour faire face à ses conséquences. L'accord étant trouvé sur ces 3 termes, leur définition et les limites qu'ils recouvrent ; l'objectif sera de ramener, par des mesures de sécurité appropriées, tous les risques au niveau « acceptable ».

MEHARI propose une grille d'aversion au risque, construite sur la base de l'appréciation du risque par rapport à son impact et à sa potentialité. Cette grille est validée par la direction générale et les départements opérationnels lors de la réunion.

I \ P	0	1	2	3	4
4	0	3	4	4	4
3	0	2	3	3	3
2	0	1	2	2	3
1	0	0	0	1	1

4 Risque insupportable
3 Risque inadmissible
Risque toléré

Tableau 2-12 : Grille d'évaluation du niveau de risque

La direction générale de « Bénin Cosmetics », au vu de ses objectifs exige, que soient assurées :

La disponibilité des moyens de communication au siège de Cotonou comme à l'usine de Parakou ;
La disponibilité de la messagerie ;
La production ;
La confidentialité et l'intégrité des secrets de fabrication, entre le siège, l'usine et le partenaire en France ;
La mise à jour des programmes de production.

II.3.2.2.2 Valeurs de l'entreprise : classification des ressources

Cette partie a pour objectif de faire une classification des ressources de l'entreprise :

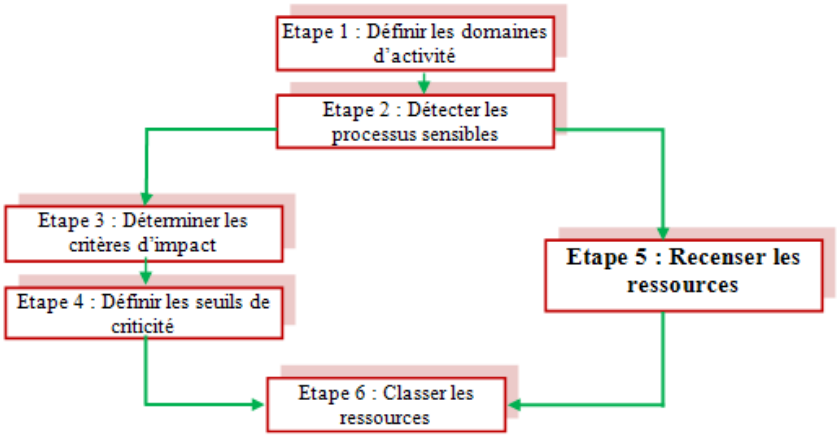


Figure 2-11 : Classification des valeurs de l'entreprise

Etape 1 : Définir les domaines d'activités et processus

La direction générale et les départements opérationnels nous ont permis de valider la cartographie des domaines fonctionnels dans le tableau des processus majeurs de l'entreprise ci-après :

DOMAINE	PROCESSUS	DESCRIPTION
Management	Prise de décisions	Ensemble des éléments contribuant à la prise de décisions (acquisition, cession, données budgétaires et prévisionnels, etc.).
Département R&D	Recherche	Travaux de recherche avancée conduisant à des nouveaux projets de produits.
Département R&D	Développement	Elaboration des processus de fabrication de nouveaux produits, et élaboration des caractéristiques des produits.
Département Production	Production	Production des produits cosmétiques, contrôle qualité, conditionnement.
Département Logistique	Logistique	Gestion de stocks, Préparation des commandes, Expédition vers le réseau de distributions franchisées.
DRH	Paie	Gestion de la paie et des comptes personnels associés (intéressement).
DRH	Frais	Gestion des frais (avances sur frais, paiement des notes de frais, etc.).
Marketing	Marketing	Recherche des éléments significatifs du marché et élaboration d'une stratégie de vente.
Finance	Comptabilité	Comptabilité générale et gestion des obligations légales afférentes (fisc, comptes sociaux, etc.)
Finance	Contentieux	Gestion du contentieux entre la logistique et la comptabilité (clients et fournisseurs).
Finance	Contrôle de gestion	Consolidation des comptes, soldes de gestion et tableau de bord.
Finance	Trésorerie	Gestion et optimisation des flux de trésorerie. Gestion des relations avec les organismes financiers et les Douanes.
Service Commercial	Commercialisation	Elaboration des outils de vente spécifiques d'un type de produit ou de service.
Service Commercial	Proposition commerciale	Elaboration de l'offre spécifique d'un client (pour les offres sur devis)
Service Commercial	Gestion des commandes	Gestion et suivi des commandes client, depuis l'offre jusqu'à la livraison (incluant ou non la maintenance).
Service Commercial	Suivi des clients	Gestion permanente des clients, de leurs particularités. Gestion des cibles commerciales.
Département informatique	Architecture exploitation informatique	Architecture réseaux & systèmes, Administration et exploitation des centres informatiques.
Département informatique	Projets informatiques	Développements d'applications informatiques. Maintenance des applications existantes.
Département informatique	Supports aux utilisateurs	Assistance aux utilisateurs, Formation, conseil

Achats	Achats	Gestion des commandes (produits et services) et des fournisseurs
Juridique	Accords et contrats	Gestion des accords et contrats. Enregistrement et conservation des pièces contractuelles.
Support	Service généraux	Ensemble des processus des services généraux, courrier, standard téléphonique, entretien, etc.

Tableau 2-13 : Domaine d'activités et processus de « Bénin Cosmetic »

Etape 2 : Détecter les processus sensibles

D'après la direction générale et les responsables des départements opérationnels de « Bénin Cosmetics), les processus critiques sont :

- « Achat » dans le domaine « Achat » ;
- « Production » dans le domaine « Département Production » ;
- « gestion des commandes » dans le domaine « Commercial » ;

Le processus « Achat » permet au responsable des achats de mieux choisir les fournisseurs de matières premières en prenant en compte les coûts, la qualité et les délais de livraison. Il en résultera pour « Bénin Cosmetics » une meilleure compétitivité et un chiffre d'affaire en conséquence.

Etape 3 : Déterminer les critères d'impact

Dans cette étape, il s'agit de demander aux responsables, quel serait l'impact sur l'entreprise en termes opérationnels, financiers ou d'image en cas de dysfonctionnement d'un des processus vitaux.

Nous définissons les critères d'impact pour les processus de chaque domaine à partir du tableau suivant :

IMPACT	
Domaines	**Description de l'impact**
Département R&D	Divulgation de plans de nouveaux produits ou de savoir-faire
Département R&D	Perte de savoir-faire
Département R&D	Non tenue des délais de développement
Département R&D	Augmentation des charges de développement
Commercial	Incapacité à exploiter des opportunités commerciales
Commercial	Perte de chiffre d'affaire
Commercial	Baisse d'efficacité commerciale
Commercial	Augmentation des charges commerciales
Commercial	Perte de compétitivité
Commercial	Perte de confiance des clients
Commercial	Incapacité à remplir des obligations contractuelles
Département Production	Non tenue des délais de production
Département Production	Augmentation des charges de production
Département Production	Perte de productivité
Département Production	Détérioration de la qualité de la production
Finance	Paiement de pénalités contractuelles
Finance	Détournement de fonds
Finance	Augmentation des charges administratives
Finance	Augmentation du risque de fraude
Juridique	Mise en examen d'un membre du Directoire
Juridique	Poursuite judiciaire de la société
Juridique	Perte de protection juridique du patrimoine

Personnel	Divulgation de renseignements concernant la vie privée
Management	Prise de mauvaises décisions de management

Tableau 2-14 : Détermination des critères d'impact

Etape 4 : Définir les seuils de criticité

Il est nécessaire, dans cette étape, d'établir les quatre seuils de criticité associés à chaque critère d'impact retenu :

Seuil 1 : Sans dommage significatif sur les opérations de « Bénin Cosmetics » ;
Seul 2 : Dommage important sur les opérations de « Bénin Cosmetics » sur la compétitivité ;
Seuil 3 : Grave dommage ne compromettant pas un domaine de « Bénin Cosmetics » ;
Seuil 4 : Dommages extrêmement graves mettant en danger la survie de « Bénin Cosmetics » ;

Nous définissons les seuils de gravité d'impact pour chaque critère d'impact retenu à partir du tableau suivant :

SEUILS D'IMPACTS
Indiquer pour chaque critère d'impact, les seuils de gravité, en se basant sur les définitions suivantes :
Gravité 1 : Impact non significatif au niveau de « Bénin Cosmetics ».
Gravité 2 : Impact significatif, résorbé facilement et rapidement.
Gravité 3 : Sinistre grave dont « Bénin Cosmetics » mettra plusieurs mois à se remettre.
Gravité 4 : Sinistre extrêmement grave menaçant la survie de « Bénin Cosmetics » ou dont elle mettra plusieurs années à se remettre.

TYPE D'IMPACT	SEUILS			
	Gravité 1	**Gravité 2**	**Gravité 3**	**Gravité 4**
Divulgation de plans de nouveaux produits ou de savoir-faire	Divulgation partielle ne permettant pas à la concurrence de rattraper son retard.	Divulgation partielle permettant à la concurrence de nous rattraper plus de 6 mois après le lancement.	Divulgation permettant à la concurrence de nous rattraper au début du lancement d'un produit stratégique (entre 0 et 6 mois).	
Perte de savoir-faire	Destruction de la copie d'un ou plusieurs fichiers d'un représentant en tournée.	Indisponibilité de la base d'informations techniques pour la maintenance, pendant une durée inférieure à 1 semaine	Destruction de l'ensemble de l'aide automatisée à la maintenance (reconstitution : plusieurs mois) ou indisponibilité > 1 semaine	Départ d'une équipe hautement spécialisée, seule capable d'assurer la maintenance d'un produit majeur de l'entreprise.
Non tenue des délais de développement	retard inférieur à un mois	retard compris entre 1 et 3 mois	retard compris entre 3 et 12 mois	Retard supérieur à 1 an
Augmentation des charges de développement	< 5 %	5% < Delta < 20%	> 20%	

Tableau 2-15 : Les seuils de gravité d'impact pour chaque critère d'impact retenu

Etape 5 : Recenser les ressources

Une fois le niveau de décomposition choisi (en fonction de la granularité d'analyse souhaitée) et après avoir confirmé les limites du domaine étudié et précisé les intentions en matière d'investigation plus ou moins poussée, nous recensons, à l'aide d'un tableau du modèle ci-après, les ressources que l'on veut classifier.

RESSOURCES
Indiquer les ressources que l'on souhaite classifier, leur type, ainsi que leur domaine et éventuellement les processus auxquels elles appartiennent.
Dans les colonnes domaines et processus, "**tous**" signifie que la ressource est unique pour tous les domaines, "**chaque**" signifie que l'on identifie une ressource différente pour chaque domaine.

NOM	TYPE	DOMAINES	PROCESSUS
Siège social Cotonou	Site et bâtiments	Tous	
Usine Parakou	Site et bâtiments	Tous	
Salle serveurs Cotonou	Locaux	Tous	
Salle serveurs Parakou	Locaux	Tous	
Centre de production Parakou	Locaux	Tous	

LAN Cotonou	Réseau	Tous	
LAN Parakou	Réseau	Tous	
Réseau public « Bénin Télécoms »	Réseau	Tous	
Serveur de stockage	Système	Tous	
Serveurs « métiers »	Système	Tous	
Serveur messagerie	Système	Tous	
SAGE SAARI	Logiciel	commercial	Tous
GES_DRH	Logiciel	Personnel	Tous
Personnel informatique	Ressource humaine		

Tableau 2-16 : Recensement des ressources

Etape 6 : Classifier les ressources

L'objectif de cette étape est de faire une classification des ressources retenues dans l'étape 5.

La classification des ressources, qui consiste à analyser si une perte de disponibilité, d'intégrité ou de confidentialité d'une ressource peut conduire à un des critères d'impacts retenus et, dans l'affirmative, à quel niveau maximum. Ce niveau est alors la classification de la ressource pour l'aspect considéré (disponibilité, intégrité ou confidentialité).

Pour chacune de ces ressources, on se pose les questions suivantes :

- Que se passerait-il si la ressource était non disponible ? (Disponibilité) ;
- Que se passerait-il si la ressource était non fiable ? (Intégrité) ;
- Que se passerait-il si la ressource était atteinte par des tiers non autorisés ? (Confidentialité) ;

Cette étape permet donc de trouver une valeur propre pour chaque ressource :

Ressource : SAGE SAARI			
Impact	Disponibilité	Intégrité	Confidentialité
Perte de chiffre d'affaire	2	2	1
Perte de confiance des clients	1	1	2
Baisse d'efficacité commerciale	2	1	1
Synthèse de classification	2	2	2

Tableau 2-17 : Détermination de la valeur propre de chaque ressource

Lors d'une réunion avec la Direction Générale et les directions opérationnelles, nous validons la classification des ressources dans le tableau de synthèse de la classification des ressources ci-après:

RESSOURCES			
NOM	**Disponibilité**	**Intégrité**	**Confidentialité**
Siège social Cotonou	1	1	2
Usine Parakou	2	1	2
Salle serveurs Cotonou	2	2	1
Salle serveurs Parakou	2	2	1
Centre de production Parakou	2	2	2
LAN Cotonou	4	4	4
LAN Parakou	4	4	4
Réseau public « Bénin Télécoms »	4	4	4
Serveur de stockage	2	2	2
Serveurs « métiers »	2	2	2
Serveur messagerie	4	4	4
SAGE SAARI	2	2	2
GES_DRH	2	2	2
Personnel informatique	2	2	2

Tableau 2-18 : Tableau de synthèse de la classification des ressources

II.3.2.2.3 La politique de sécurité

La politique de sécurité du système d'information ne peut s'élaborer correctement et efficacement si elle ne tient pas compte de la stratégie globale de sécurité de « Bénin Cosmetics ». La politique de sécurité se base sur des normes nationales et internationales tout en restant en conformité avec les législations en vigueur dans le pays.

« Bénin Cosmetics » ne dispose pas d'une politique de sécurité

II.3.2.2.4 La charte de management

Au cours d'une réunion avec le staff managérial de « Bénin Cosmetics », il nous présente sa « Charte Managériale pour l'usage des ressources Informatiques et des services Internet à l'entreprise Bénin Cosmetics »

Cette charte devrait permettre :

- De renforcer la sécurité des systèmes d'informations en informant et en responsabilisant les utilisateurs ;
- De préciser les prérogatives et le cadre de travail de chaque type d'acteur pour éviter des actions dangereuses voire illégales, pouvant engager la responsabilité civile ou pénale de leurs auteurs et/ou de la direction générale et le département informatique ;
- De vous mettre en conformité avec la loi.

Cette charte doit également informer les utilisateurs de l'existence de dispositifs de contrôle et d'éventuelles sanctions.

II.3.2.3 Plan opérationnel de sécurité

Le plan opérationnel doit obligatoirement être précédé d'un plan stratégique dans la mesure où la définition d'une métrique des risques et une classification des ressources sont indispensables, quelle que soit l'importance de l'entreprise considérée, à l'évaluation des risques et à la détermination objective des besoins en services de sécurité. L'élaboration d'un plan opérationnel de sécurité résulte soit :

- De la décision d'une unité indépendante ou d'un responsable d'activité (cas des petites entreprises, professions libérales, etc.). Dans ce cas, on peut considérer que, bien que faisant l'objet d'étapes préalables spécifiques (impérativement la définition de la métrique des risques et la classification des ressources), le plan stratégique sera pratiquement intégré dans le plan opérationnel ;
- de la décision d'une unité autonome, qui devra se plier aux exigences définies dans le plan stratégique aux fins de coordination et de cohérence ;
- de la mise en œuvre de la politique de sécurité décidée au niveau central et dont le plan opérationnel est un des composants.

Le plan opérationnel peut être élaboré :

- soit à partir d'une approche analytique basée sur un audit des services de sécurité en place assuré principalement, parce que ce sont eux qui en ont la meilleure connaissance, par des techniciens ;

- soit à partir d'une évaluation des facteurs de risque, c'est à dire d'une appréciation de leur incidence sur la gravité du risque. Une telle approche globale, fait d'abord appel à l'appréciation et au raisonnement des utilisateurs des systèmes informatiques.

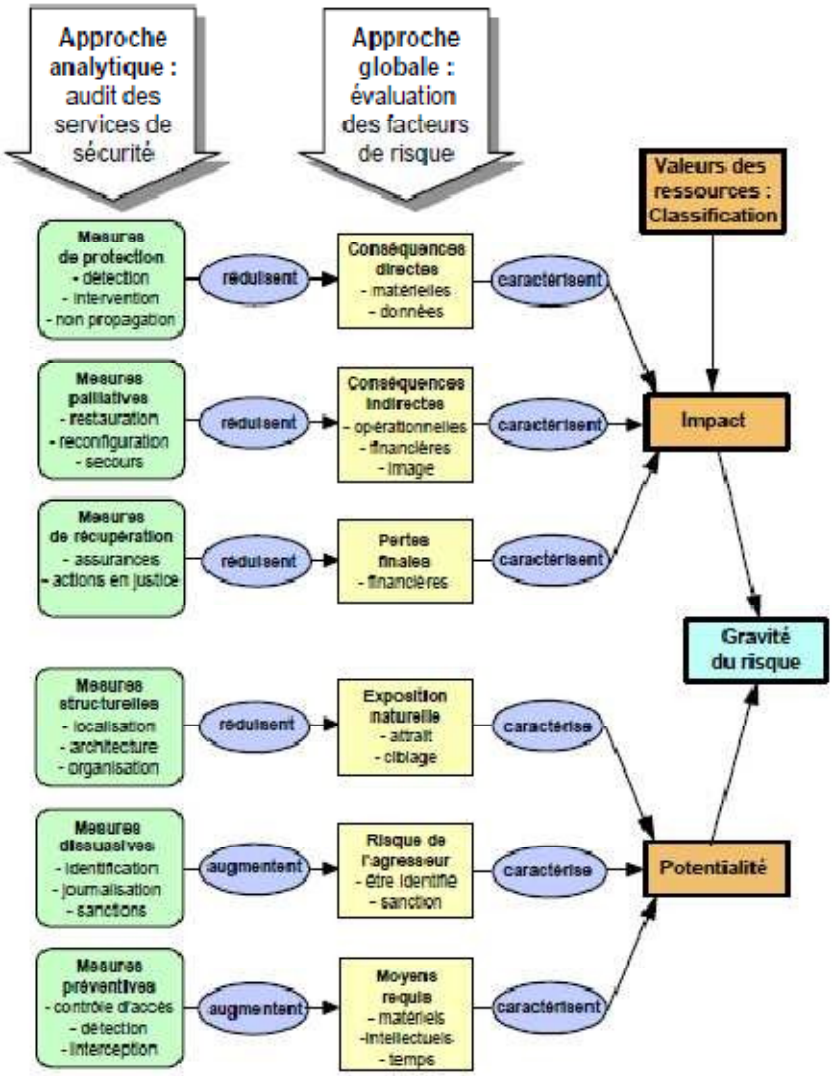


Figure 2-12 : Elaboration du plan de sécurité

II.3.2.3.1 Préliminaires

Etape 1 : Définition du domaine couvert ou périmètre de l'étude

Sur recommandation de la Direction Générale de « Bénin Cosmetics », le domaine couvert par l'étude est :

- Les 2 sites de l'entreprise à Cotonou et à Parakou ;
- Les locaux techniques du siège à Cotonou et à Parakou ;
- Le centre de production à Parakou ;
- Les réseaux locaux du siège à Cotonou et du centre de production à Parakou ;
- Réseau public « Bénin Télécoms » ;
- Les serveurs ;
- Les applications SAGE SAARI et GES_DRH ;

Etape 2 : réalisation de la décomposition cellulaire

Au sein d'une organisation comme « Bénin Cosmetics » qui est repartie en plusieurs sites et plusieurs systèmes informatiques, les résultats d'audits sont forcément différents selon les éléments mis en jeu. La réalisation de notre audit a mis en lumière toutes ces différences afin d'avoir une vue réelle de la vulnérabilité des systèmes existants. Cette tâche nous a été facilitée par la décomposition cellulaire.

Les services de sécurité sont rassemblés dans les types de cellules au niveau de la base de connaissances, ce qui facilite l'identification du profil des répondants (un type de cellule rassemblant les questions destinées à un profil de répondant).

Nous avons retenu pour l'entreprise « Bénin Cosmetics » la décomposition suivante :

- Entité : Entreprise « Bénin Cosmetics » ;
- Sites : Siège à Cotonou, usine à Parakou ;
- Locaux : local technique siège, local technique usine Parakou, centre de production, bureaux sièges Cotonou, bureaux usine Parakou ;
- Architecture réseaux et télécom : LAN siège Cotonou, LAN usine Parakou, réseau étendu « Bénin Télécoms » ;
- Exploitation réseaux et télécoms : exploitation des réseaux téléphoniques ;
- Architecture des systèmes : serveur métier, serveur de stockage, serveur de messagerie ;
- Applications opérationnelles : application SAGE SAARI, GES_DRH ;

La décomposition cellulaire est une étape déterminante pour l'étude des risques. Elle se fait très souvent à l'aide d'outils comme RISICARE qui automatise aussi l'étude des risques.

A. **Domaine de l'organisation de la sécurité** : Entreprise « Bénin Cosmetics »
B. **Domaine lié au site et à l'établissement** : siège à Cotonou et usine à Parakou
C. **Domaine de la protection des locaux** : local technique à Cotonou, local technique à Parakou, centre de production à Parakou, bureaux du siège à Cotonou, bureaux usine à Parakou ;
D. **Domaine de l'architecture réseau et télécoms** : LAN de Cotonou, LAN de Parakou, réseau étendu de « Bénin Telecoms »
E. **Domaine de la sécurité de l'exploitation des réseaux** : exploitation des réseaux téléphoniques
F. **Domaine de la sécurité des systèmes et leur architecture** : serveur de stockage, serveur métier, serveur de messagerie
G. **Domaine de la sécurité de la sécurité applicative** : Application SAGE SAARI, application GES_DRH
H. **Domaine de la sécurité dans les développements** : Développement GES_DRH

Tableau 2-19 : Décomposition cellulaire de l'entreprise

Etape 3 : Reprise de la classification

Nous avons repris la classification des cellules en fonction des trois critères d'impact : disponibilité (D), intégrité (I), confidentialité (C). Chaque cellule s'est vue affectée d'une valeur indiquant son degré de criticité par rapport à un critère donné.

A. **Domaine de l'organisation de la sécurité** : Entreprise « Bénin Cosmetics »
B. **Domaine lié au site et à l'établissement** : siège à Cotonou (1, 1,2) et usine à Parakou (2, 1,2)
C. **Domaine de la protection des locaux** : local technique à Cotonou (4, 4,4), local technique à Parakou (4, 4,4), centre de production à Parakou (2, 2,1), bureaux du siège à Cotonou, bureaux usine à Parakou ;
D. **Domaine de l'architecture réseaux et télécoms** : LAN de Cotonou (4, 4,4), LAN de Parakou (4, 4,4), réseau étendu de « Bénin Telecoms » (4, 4,4)

E. **Domaine de la sécurité de l'exploitation des réseaux** : exploitation des réseaux téléphoniques (4, 4,4)
F. **Domaine de la sécurité des systèmes et leur architecture** : serveur de stockage (2, 2,2), serveur métier 2, 2,2), serveur de messagerie (4, 4,4)
G. **Domaine de la sécurité applicative** : Application SAGE SAARI (2, 2,2), application GES_DRH (2, 2,2)
H. **Domaine de la sécurité dans les développements** : Développement GES_DRH (2, 2,2)

Tableau 2-20 : Classification des cellules en fonction des critères d'impact

II.3.2.3.2 Audit de l'existant

L'audit de l'existant se décompose en deux épreuves : la réalisation de l'audit et la production des résultats de l'audit.

Pour chaque cellule, il fallait rencontrer la ou les personnes concernées par celles-ci et ayant le profil associé au type de cellule auquel appartient cette cellule.

Pour une question de pertinence, nous avons porté notre préférence sur des questions dichotomiques. Ce qui implique que le répondant doit indiquer une réponse OUI ou NON pour chaque question (en cas d'hésitation ou de réponse partiellement affirmative, on a choisi de répondre NON par prudence). Nous avons aussi donné la possibilité de choisir S.O pour sans objet au cas où les questions d'audit ne concernent pas l'étude.

La production des résultats de l'audit passe par une consolidation des réponses en vue d'obtenir une note pour le sous service auquel elles appartiennent. Ce calcul fait intervenir une moyenne pondérée normée de 0 à 4 plus, éventuellement, une notion de seuil maximum et minimum.

Le seuil Max est utilisé pour les questions indispensables au sein d'un sous service, il correspond à la limite maximum de niveau de qualité que peut atteindre le sous service lorsqu'on a répondu Non à ces questions.

A l'inverse le seuil Min est utilisé pour les questions suffisantes au sein d'un sous service, il correspond à la note minimale atteinte lorsqu'on a répondu Oui à ces questions.

Naturellement si plusieurs questions au sein d'un sous service déclenchent des seuils Max différents, on retiendra le seuil MAX le plus faible.

A l'inverse si plusieurs questions au sein d'un sous service déclenchent des seuils Min différents, on retiendra le seuil MIN le plus élevé.

En cas de conflit entre seuils MAX et MIN (c'est à dire un déclenchement de seuil MAX de valeur inférieure à celle d'un déclenchement de seuil MIN), c'est le seuil MAX qui prévaudra.

Ces résultats d'audit peuvent être utilisés pour produire des tableaux de vulnérabilité pour chacune des cellules.

QUESTIONNAIRE D'AUDIT : DOMAINE DES LOCAUX

Question	Rép.	P	Max	Min	Commentaire
Qualité de la fourniture d'énergie					
L'énergie électrique fournie répond-elle aux exigences maximales spécifiées par les fournisseurs d'équipements avec une marge suffisante ?		2			
Y a-t-il un système de régulation électrique comportant au moins un onduleur pour les équipements sensibles ?		4			
Continuité de la fourniture de l'énergie					
Existe-t-il une installation électrique de secours capable d'assurer la continuité du service des équipements critiques (s'appuyant sur un groupe électrogène associé à une réserve de carburant suffisante ou sur des arrivées indépendantes d'énergie) ?		4			
Teste-t-on régulièrement la capacité du système de secours à assurer la charge prévue (les délestages éventuels ayant été effectués) ?		4			

Sécurité de la climatisation					
Y a-t-il un système de climatisation créant une ambiance (température, hygrométrie, poussières) conforme aux prescriptions des constructeurs des matériels installés ?		4			
Vérifie-t-on régulièrement la capacité du système de climatisation à assurer sa fonction dans les pires conditions climatiques envisageables ?		4			
Protection contre la foudre					
L'immeuble est-il protégé par un paratonnerre ?		4			
Les circuits électriques et le câblage sont-ils protégés contre les surtensions et contre la foudre par des équipements spéciaux ?		4			
Contrôle d'accès aux locaux sensibles					
Les droits d'accès permanents ou semi-permanents (pour une durée déterminée) aux locaux sensibles sont-ils définis par rapport à des "profils" types prenant en compte la fonction et le statut (personnel d'exploitation informatique ou télécom, personnels des services généraux ou de sécurité, pompiers, prestataires de maintenance ou d'entretien, fournisseurs de services, stagiaires, visiteurs, etc.) ?		4			
Les profils permettent-ils également de définir des créneaux horaires et calendaires de travail (heures début et fin de journée, week-end, vacances, etc.) ?		4			
Les badges ou cartes matérialisant les autorisations d'accès aux locaux sensibles sont-ils personnalisés avec le nom du titulaire et sa photo ?		4			
Utilise-t-on un système de contrôle d'accès systématique aux locaux sensibles ?		4			
L'authentification fait-elle appel à des moyens infalsifiables détenus par l'utilisateur (carte à puce ou reconnaissance biométrique, par exemple) ?		4			
Le système de contrôle d'accès garantit-il un contrôle exhaustif de toute personne entrant dans les locaux (SAS ne permettant le passage que d'une personne à la fois, processus interdisant l'utilisation du même badge par plusieurs personnes, etc.) ?		4			
Sécurité incendie					
A-t-on fait une analyse systématique et approfondie de tous les risques d'incendie (court-circuit au niveau du câblage, effet de la foudre, personnel fumant dans les locaux, appareillages électriques courants, échauffement d'équipement, propagation depuis l'extérieur, propagation par les gaines techniques ou la climatisation, etc.) ?		4			
Existe-t-il une installation de détection automatique d'incendie complète pour les locaux sensibles (faux planchers et faux plafonds s'ils existent) ?		2			
L'installation de détection est-elle composée d'au moins deux types de détecteurs (par exemple : détecteurs de fumée ioniques et optiques) ?		4			
Le poste de surveillance a-t-il la possibilité de faire intervenir rapidement une équipe d'intervention ayant les moyens d'action suffisants pour agir (diagnostic précis de la situation, extinction manuelle, déclenchement ou validation de l'extinction automatique, appel des secours, etc.) ?		2			

Tableau 2-21 : Extraits du questionnaire d'audit des locaux

QUESTIONNAIRE D'AUDIT : DOMAINE DU RESEAU LOCAL					
Question	Rép.	P	Max	Min	Commentaire
Sécurité de l'architecture du réseau local					
A-t-on effectué un partitionnement du réseau local en séparant du réseau strictement interne les zones de communication avec l'extérieur (DMZ) ?		4			
A-t-on effectué un partitionnement du réseau local en domaines de sécurité correspondant à des exigences de sécurité homogènes et à des espaces de confiance à l'intérieur desquels les contrôles peuvent être adaptés ?		4			
En particulier tout réseau sans fil (Wlan) est-il considéré comme un domaine distinct strictement isolé du reste du réseau (par firewall, routeur filtrant, etc.) ?		4			
A-t-on effectué un partitionnement du réseau local en domaines de sécurité correspondant à des exigences de sécurité homogènes et à des espaces de confiance à l'intérieur desquels les contrôles peuvent être adaptés ?		4			

Sûreté de fonctionnement des éléments d'architecture du réseau local					
A-t-on analysé chaque domaine de sécurité pour déterminer les exigences de continuité de service et en a-t-on déduit, si nécessaire, une architecture de redondance au niveau des points d'interconnexion, des équipements et du maillage du réseau ?		4			
L'architecture des équipements de réseau permet-elle une adaptation facile aux évolutions de charge (clusters, grappes, etc.) ?		4			
Organisation de la maintenance des équipements du réseau local					
Tous les équipements du réseau local sont-ils couverts par un contrat de maintenance ?		2			
A-t-on identifié les équipements critiques pour l'exploitation et la tenue des performances annoncées et, pour ceux-ci, les délais de remise en service souhaitable et les délais maximum tolérables en cas de défaillance ?		4			
Procédures et plans de reprise du réseau local sur incidents					
A-t-on établi une liste des incidents pouvant affecter le bon fonctionnement du réseau local et, pour chacun d'eux, la solution à mettre en œuvre et les opérations à mener par le personnel d'exploitation ?		2			
Les moyens de diagnostic d'une part et de pilotage du réseau local (reconfiguration) d'autre part couvrent-ils de manière satisfaisante tous les cas de figures analysés et permettent-ils de mettre en œuvre les solutions décidées dans les délais spécifiés ?		4			
A-t-on défini, pour chaque incident réseau, un délai de résolution et une procédure d'escalade en cas d'insuccès ou de retard des mesures prévues ?		4			
Plan de sauvegarde des configurations du réseau local					
A-t-on établi un plan de sauvegarde, couvrant l'ensemble des configurations du réseau local, définissant les objets à sauvegarder et la fréquence des sauvegardes ?		4			
Ce plan de sauvegarde est-il traduit en automatismes de production ?		4			
Teste-t-on régulièrement que les sauvegardes des programmes (sources et/ou exécutables), de leur documentation et de leur paramétrage permettent effectivement de reconstituer à tout moment l'environnement de production ?		4			
Plan de Reprise d'Activité (PRA) du réseau local					
Existe-t-il une solution de secours, parfaitement opérationnelle, pour pallier l'indisponibilité de tout équipement ou de toute liaison critique ?		4			
Ces solutions sont-elles décrites en détail dans des Plans de Reprise d'Activité incluant les règles de déclenchement, les actions à mener, les priorités, les acteurs à mobiliser et leurs coordonnées ?		4			
Ces plans sont-ils testés de manière opérationnelle au moins une fois par an ?		4			

Tableau 2-22 : Extraits du questionnaire d'audit du réseau local

Ces tableaux et graphiques nous permettent de faire un reporting sur la vulnérabilité de la société. Bien que ce ne soit pas la finalité de la méthode Méhari, cela nous facilite la comparaison de diverses cellules du même type et nous permettra un suivi dans le temps de cette vulnérabilité.

II.3.2.3.3 Evaluation de la gravité des scénarii

La base de connaissances Méhari offre une liste de scénarii types ainsi que les six formules indiquant les sous services utilisés pour chaque type de mesure (Structurelle, Dissuasive, Préventive, de Protection, Palliative, de Récupération).

06	**Altération des données**						
	10	**Accident de traitement**					
		11	Accident d'exploitation			I	N
			Stru	Diss	Prév		
			Min (01B05 ; 01C01)		Max (06D01 ; min (07A05 ; 07D03))		
			Prot	Pall	Récup		
			Min (08B04 ; 07E03)	Min (07D05 ; 08D02)	Min (01D02 ; 01D05)		
		12	Altération accidentelle des données pendant la maintenance			I	N

			Stru	Diss	Prév		
			Min (01B05 ; 01C01)		Max (07A05 ; 09C01)		
			Prot	Pall	Récup		
			Min (08B04 ; 07E03)	Min (07D05 ; 08D02)	Min (01D02 ; 01D05)		
	20	**Erreur de saisie**					
		21	En amont de la saisie			I	E
			Stru	Diss	Prév		
			Min (01B05 ; 01C01)		08B03		
			Prot	Pall	Récup		
			08B04	Min (07D05 ; 08D02)	Min (01D02 ; 01D05)		
		22	Lors de la saisie			I	E
			Stru	Diss	Prév		
			Min (01B05 ; 01C01)		08B03		
			Prot	Pall	Récup		
			08B04	Min (07D05 ; 08D02)	Min (01D02 ; 01D05)		

Tableau 2-23 : Extraits de l'évaluation de la gravité des scénarii (source CLUSIF 2007 – Base des connaissances)

Pour illustration, les scénarii 6.22 qui concerne l'altération de données ayant pour cause une erreur de saisie de données et pour origine, nous avons quantifié les mesures structurelles par la formule : Min (01B05 ; 01C01), cela signifie que les sous services 01B05 : « Sensibiliser et former à la sécurité » et 01C01: "Motiver le personnel" sont impliqués dans la quantification de ces mesures structurelles.

En se penchant su l'ensemble des sous services de la base des connaissances Méhari 2007 impliqués dans la quantification des six types de mesures pour ce scénario, le constat qui se dégage est qu'ils appartiennent au type de cellule Entité, Production Informatique et Sécurité Applicative, nous dirons que ce scénario s'appuie sur ces trois types de cellules pour se réaliser.

Pour un scénario type et les cellules associées (par exemple le scénario 622 du tableau précédent se réalisant dans les cellules Entité et Production Informatique et Sécurité Applicative), on calcule pour chaque type de mesure (Structurelle, Dissuasive, Préventive, de Protection, Palliative de Récupération), l'efficacité de celle-ci : Eff-Stru, Eff-D iss, Eff-Prev, Eff-Prot, Eff-Recup. Pour cela, on utilise les formules associées à chaque type de mesure du scénario type étudié.

Réplication du scénario dans les cellules

Code	Domaine de l'organisation	Domaine de la sécurité des serveurs	Domaine de la sécurité des applications	expo	Diss	Prev	Prot	Pall	Recup	P	RI	GMax
0622/1	Entreprise « Bénin Cosmetics »	Exploitation des serveurs	Application SAGE SAARI	1	-	2	2	2	4	2	3	2
0622/2	Entreprise « Bénin Cosmetics »	Exploitation des serveurs	Application GES_DRH	1	-	2	2	2	4	2	3	2

Tableau 2-24 : Extrait du tableau du calcul des statuts détaillés

On déduit la potentialité STATUS-P à partir des trois statuts de potentialité (STATUS-EXPO, STATUS-DISS, STATUS-PREV) en utilisant la grille correspondant au type de scénario (P-MALVEILLANCE, P-ERREUR, P-ACCIDENT).

Le scénario 06.22 : " Altération de données par erreur lors de la saisie " est de type Erreur.

II.3.2.3.4 Expression des besoins de sécurité

Les besoins de sécurité sont déduits de l'évaluation de la gravité des scénarii et de l'appréciation, aussi objective que possible des services de sécurité ayant une influence sur cette gravité.

Les principaux soucis de tous les acteurs de la sécurité est naturellement de réduire à leur strict minium les risques insurmontables (en priorité) puis inadmissibles, jusqu'à ce que le niveau du sinistre potentiel passe sous la barre du seuil fixé comme ne devant pas être franchi. L'expression des besoins de sécurité sera donc, d'abord, l'expression des besoins de mesures spécifiques répondant aux risques majeurs (insupportables puis inadmissibles) découlant de l'étude des scénarii les plus graves.

Mais, s'il est crucial de réduire ces risques majeurs, il est également impératif de veiller à ce que chaque entité applique des mesures de sécurité générale qui soient conformes aux choix définis par la politique de l'entreprise et répondent à ses risques courants. C'est pourquoi l'expression des besoins se traduira, outre la mise en place des mesures spécifiques au domaine étudié, par un ensemble de mesures résultant d'une comparaison entre le niveau de qualité des mesures en place et le niveau spécifié par la politique de sécurité de l'entreprise.

Mesures générales pour la cellule exploitation des serveurs		
Note	**Code**	**Sous service**
2.0	07A02	Sécurité des impressions
2.0	07D02	Organisation de la maintenance
2.4	07E02	Traitement des incidents
3.0	07A07	Contrôle de la télémaintenance
3.0	07A08	Administration des serveurs
3.2	07A01	Contrats de service

Tableau 2-25 : Extrait du tableau de l'expression des besoins de sécurité de la cellule exploitation des serveurs

Mesures générales pour la cellule sécurité applicative		
Note	**Code**	**Sous service**
2.0	07A02	Reconfiguration logicielle
2.0	07D02	Identification de l'origine (signature…)
2.0	07E02	Localisation d'un événement dans le temps (horodatage)
3.0	07A07	Notarisation (anti-répudiation)

Tableau 2-26 : Extrait du tableau de l'expression des besoins de sécurité de la cellule sécurité application GES_DRH

Pour élaborer le plan d'action des mesures générales, nous prendrons en compte les contraintes organisationnelles, techniques mais aussi financières. Pour l'ensemble des mesures générales nous pourrons traiter les sous services utilisant des aspects légaux ou réglementaires (preuve et contrôle, traçabilité, auditabilité, …).

Pour mener cette étude concernant « Bénin Cosmetics », nous avons traité les sous services suivants :

- 08F01 Identification de l'origine (signature, ….) ;
- 08F06 Localisation d'un événement dans le temps (horodatage, …),
- 08F05 Notarisation (anti-répudiation)

II.3.2.4 Plan opérationnel d'entreprise

Le Plan Opérationnel d'Entreprise (POE) est la consolidation des actions de sécurité engagées dans chaque unité. C'est dans cette phase que l'on doit positionner des indicateurs de sécurité pour suivre l'évolution du niveau de sécurité globale de l'entreprise. Ces indicateurs permettront de surveiller les points sensibles ou névralgiques de l'entreprise et à la Direction Générale de suivre l'évolution du niveau global de sécurité en fonction de objectifs définis.

Le POE donnera lieu à l'établissement d'un tableau de bord et pourra aussi être l'occasion d'un équilibrage entre les unités de l'entreprise.

Si de nouveaux besoins apparaissent (en raison de la vie même de l'entreprise) la politique et les objectifs de sécurité doivent être modifiés et les phases 1 à 3 réitérées.

II.3.2.4.1 Choix d'indicateurs représentatifs

En raison des objectifs de sécurité que nous a fixé la Direction Générale au niveau de l'élaboration du plan stratégique de la sécurité, le choix des indicateurs portera sur les scénarii suivants :

- Pour assurer la production :

01.12	Départ de personnel stratégique d'exploitation *Ce scénario concerne directement les ressources humaines*
02.21	Incendie dans une corbeille à papier *Ce scénario concerne directement les locaux*

Tableau 2-27 : Choix des indicateurs représentatifs de la production

- Pour assurer la confidentialité et le secret de fabrication :

05.14	Bombe logique dans un logiciel par un utilisateur *Ce scénario concerne directement les traitements informatiques*
10.51	Perte de fichiers par vol dans un bureau *Ce scénario concerne directement les structures support*

Tableau 2-28 : Choix des indicateurs représentatifs de la confidentialité et le secret de fabrication

- Pour assurer la disponibilité des moyens de communications avec l'usine de Parakou :

01.23	Accidents ou panne grave rendant indisponible une ressource matérielle informatique (serveur, réseau, LAN, WAN, etc.) *Ce scénario concerne directement les traitements informatiques*

Tableau 2-29 : Choix des indicateurs pour assurer la disponibilité des communications avec l'usine de Parakou

II.3.2.4.2 Elaboration d'un tableau de bord de la sécurité de l'entreprise

Le tableau de bord pourra permettre d'apprécier par exemple la gravité des scénarii retenus à l'étape précédente. L'appréciation du niveau de cette gravité sera réactualisée à une fréquence déterminée par l'entreprise

Famille	Libellé de la famille de scénarii	Gravité initiale	Gravité finale
02	Destruction d'équipements	3	2
03	Performances dégradées	3	2
08	Divulgation des données	3	2
09	Détournement des fichiers de données	3	3

12	Poursuite judiciaire	3	3

Tableau 2-30 : Gravité initiale et gravité finale par famille de scénarii

D'autre tableau de bord avec des indicateurs spécifiques avec le temps d'indisponibilité et/ou retour à une situation normale pourra être fourni vers la direction sous la forme suivante :

ENTREPRISE « BENIN COSMETICS »	09/2008		10/2008	
	Nombre	Temps	Nombre	Temps
Nombre d'incidents liés au mot de passe	8	4	7	3
Nombre de tentatives infructueuses de connexions sur le système	5	5	9	10
Nombre de tentatives d'intrusion	6	3	2	2
Nombre de blocage du logiciel métier	10	15	12	19
Nombre de restauration de données	10	10	2	3
Nombre de virus ayant infecté la messagerie, le S.I.	27	50	10	21

Tableau 2-31 : Tableau de bord des indicateurs spécifiques avec le temps d'indisponibilité et retour à une situation normale

II.3.2.4.3 Rééquilibrages et arbitrages entre les unités

Les rééquilibrages et les arbitrages budgétaires entre les unités seront déterminés en fonction des ressources (humaines et financières) disponibles que l'entreprise peut accorder aux différentes unités pour mettre en œuvre les plans opérationnels de sécurité.

II.3.2.4.4 Synthèse

La mise en place d'une démarche sécuritaire basée sur MEHARI est de nos jours une des plus fiables dès lors qu'elle est menée avec une volonté de l'instance managériale de l'entreprise. La sécurité ne peut se concevoir sans une maitrise réelle des risques encourus par l'entreprise et ses valeurs. La base de connaissance et des scénarii de risques prédéfinies facilitent l'identification des risques. La division des processus en cellule permet une évaluation des risques à une échelle infinie.

La démarche MEHARI est certes assez harassante et exige un véritable audit du système d'information concerné, mais elle a l'avantage d'être bien documentée et régulièrement mise à jour par le Clusif.

Chapitre 3 : Les systèmes de protection contre les intrusions

Dans le langage courant, une intrusion est une action visant à s'introduire sans autorisation dans un lieu dont on n'est pas le propriétaire. En Informatique aussi la même définition est applicable ; elle signifie la pénétration des systèmes d'information, mais aussi les tentatives des utilisateurs locaux d'accéder à de plus haut privilèges que ceux qui leur sont attribués, ou tentatives des administrateurs d'abuser de leurs privilèges. Elle peut aussi résulter d'un ver cherchant à assurer sa propagation, ou encore d'une attaque automatisée.

Les deux premières parties de ce document ont traité des évolutions de la sécurité informatique, d'un état des lieux de la sécurité des systèmes d'information dans le monde et des stratégies de sécurité des systèmes d'information qui sont d'usage pour se mettre à l'abri des menaces courantes. Cependant, le rapport menaces / mesures, loin d'être satisfaisant demeure toujours une préoccupation majeure pour les organisations et les spécialistes de la sécurité des systèmes d'information.

En effet, beaucoup de spécialistes s'accordent avec Natalie Dagorn pour clamer qu' «aucun système d'information n'est sûr à 100%! Parmi les préceptes connus sur la sécurité informatique se trouve celui énonçant que, pour une entreprise connectée à l'Internet, le problème aujourd'hui n'est plus de savoir si elle va se faire attaquer, mais quand cela va arriver ; une solution possible est alors d'essayer de repousser les risques dans le temps par la mise en œuvre de divers moyens destinés à augmenter le niveau de sécurité » [DAG].

Les vulnérabilités en matière de sécurité s'intensifient d'année en année. Le Centre de coordination CERT indique que 417 vulnérabilités ont été signalées en 1999. Au cours des trois premiers trimestres 2002, ce chiffre est monté jusqu'à 3222.

En 2006 ce même chiffre était passé à 8 064. En cette année 2008, rien que pour le premier semestre le nombre de 4 110 vulnérabilités a déjà été dépassé [CRTV].

À l'heure où les correctifs logiciels ne peuvent être appliqués aussi vite que la technologie évolue, deux questions doivent être posées : combien coûte les temps d'indisponibilité, et quel est le degré de nuisance provoqué par la compromission des données ?

Par ailleurs, une nouvelle inquiétude grandit : le fait que les entreprises soient potentiellement responsables des dégâts provoqués par un pirate et doivent prouver à la justice qu'elles ont pris les mesures nécessaires pour se défendre contre les attaques.

Au regard de ce tableau inquiétant de la sécurité informatique, les éditeurs et spécialistes des solutions de sécurité ont bien évidemment réagit en concevant des systèmes ou dispositifs capables de proscrire les dangers que ne peuvent empêcher les antivirus, pare-feux et autres mesures classiques de sécurité jusque-là en vogue.

Dans cette troisième partie, nous allons aborder les systèmes de protection contre les intrusions. En effet, nous montrerons grâce à une enquête que nous avons réalisée, que ces systèmes qui ajoutent un niveau supplémentaire de sécurité aux SI sont méconnus et négligés au sein des entreprises et organisations ouest africaines.

III.1 Situation de la sécurité des systèmes d'information dans la sous-région Ouest africaine

Le but de ce document étant de montrer l'importance et la mise en place des stratégies et politiques de sécurité, il nous a semblé opportun de compléter les études et sondages utilisés dans la première partie par une enquête beaucoup plus ciblée. Elle concerne la sous-région Ouest africaine. Nous avons porté notre choix sur 29 organisations du Bénin, Niger et du Togo. L'enquête a porté principalement sur des questions mettant de coté les mesures classiques de sécurité telles que les pare-feux et les réseaux privés virtuels. Le tableau suivant montre les entreprises concernées par l'enquête :

BENIN	NIGER	TOGO
Bénin Télécom	SONITEL	Togo Télécom
MTN Bénin SA	COMINAK (AREVA Niger)	TOGOCEL
MOOV Bénin SA	ZAIN (CELTEL)	MOOV Togo SA
Banque ATLANTIQUE Bénin SA	SAHEL COM	Banque ATLANTIQUE Bénin SA
ECOBANK Bénin SA	DUNE Télécom	ECOBANK Bénin SA
GLO Mobile Bénin SA	IX-COM	UTB
PHARAON	LIPTINFOR	Banque Populaire
COMMUNITEC		BTD
CPPE		IPNET EXPERT
IS Télécom		CAFE INFORMATIQUE
ISOCEL		IDS Technologies

Tableau 3-1 : Les entreprises Ouest-africaines concernées par l'enquête

La première question de cette enquête auprès de ces entreprises était : « Disposez-vous d'une stratégie de sauvegarde hors-site (Backup off-site) ? »

Une véritable stratégie de sauvegarde doit ressembler à celle mise en place par AfriNIC (registre africain d'Internet) qui ayant son siège principal à Johannesburg (Afrique du Sud) dispose d'un site de réplication de ses données au Caire (Egypte). C'est le concept du Backup off-site, car ces deux endroits sont géographiquement assez éloignés pour qu'une catastrophe naturelle même importante ne puisse priver AfriNIC de ses ressources. Les sauvegardes sont quotidiennement effectuées en ligne.

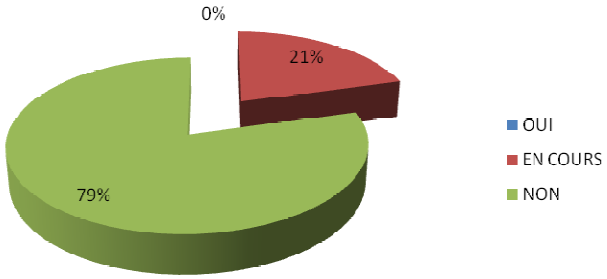


Figure 3-1 : Entreprises disposant d'une stratégie de Backup off-site

A cette question, comme le montre la figure 3-2, 79% de notre échantillon a répondu « NON » et seuls 21% disent être entrain de planifier ces mesures ne serait-ce qu'à l'échelle d'une ville ou d'un pays.

La seconde question de l'enquête se présentait comme suit : « Disposez-vous d'une démarche sécuritaire conduisant à une véritable stratégie puis politique de sécurité fiable ? ».

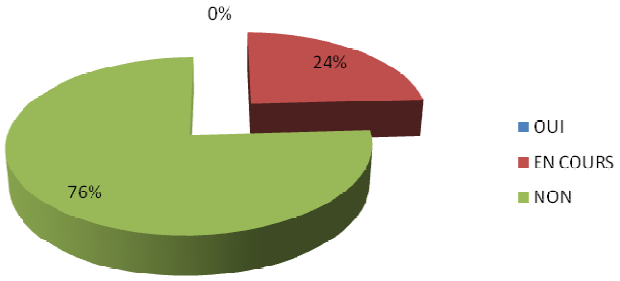


Figure 3-2 : Pourcentage des réponses au sujet de la démarche sécuritaire.

Seuls 24% des entreprises ont estimé être sur le point de le faire ou de commencer les étapes préliminaires à sa mise en œuvre. 76% ont répondu « NON ».

La troisième question était ::« Disposez-vous d'un dispositif vous permettant de vous rendre compte d'une intrusion n'ayant pas causé de dégâts, mais qui a pu occasionner vol de données ? ».

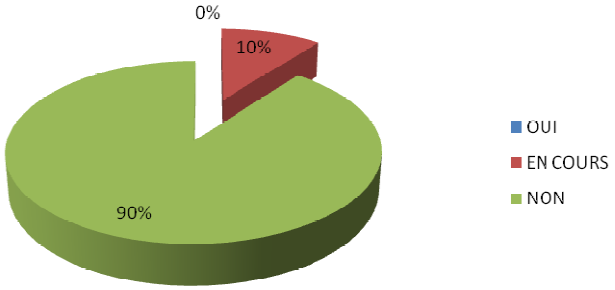


Figure 3-3 : Pourcentage de la capacité de détection des intrusions « passives »

Pour continuer avec les intrusions, nous avons aussi demandé si elles peuvent prévenir ou arrêter en temps réel une intrusion occasionnant des dommages tels que des dénis de services ? Tous les répondants ont reconnu n'être pas préparés à ces types d'attaques comme le montre la figure 3-5.

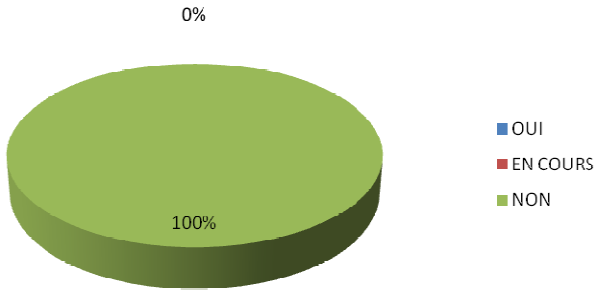


Figure 3-4 : Pourcentage de protection contre les intrusions « actives »

Enfin, la dernière question était : « Disposez-vous d'un plan de reprise d'activité après un sinistre (Disaster Recovery Plan) ? ».

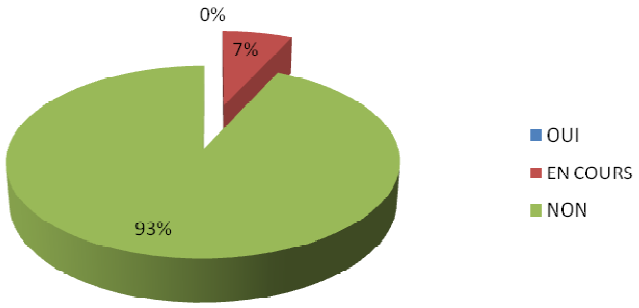


Figure 3-5 : Pourcentage des entreprises disposant d'un Disaster Recovery Plan

A cette question aussi la majorité des entreprises c'est-à-dire 93% ont répondu par la négative. Seuls 7% disent y avoir pensé.

Le constat que nous pouvons tirer de cette étude est que nos entreprises ne sont pas du tout préparées à faire face aux réels risques auxquels elles s'exposent surtout en ce qui concerne les intrusions et les attaques ciblées. C'est pourquoi, nous nous sommes proposé de terminer cette étude par la présentation d'un type assez récent de système de protection que nos entreprises devraient inclure dans leurs stratégies et politiques de sécurité à savoir les systèmes de protection contre les intrusions.

III.2 Concepts des systèmes de protection contre les intrusions

III.2.1 Définition et principes de fonctionnement

On entend par systèmes de protection contre les intrusions les logiciels ou « appliances » (c'est-à-dire des boîtes noires) capables de protéger les réseaux et systèmes informatiques contre les intrusions. Comme nous l'avons mentionné précédemment, ces systèmes se basent surtout sur les différentes techniques de détection d'intrusions qui existent aujourd'hui.

Ainsi, il existe des systèmes de détection d'intrusions dits « passifs » qui ont été déployés de plus en plus largement et qui sont aujourd'hui laissés la place aux systèmes dits « actifs » de prévention d'intrusions. La recherche et les découvertes en détection et prévention d'intrusions sont toujours d'actualité, notamment en raison des évolutions rapides et incessantes des technologies des systèmes d'information.

La détection d'intrusions peut se définir comme l'ensemble des pratiques et des mécanismes utilisés qui permettent de détecter les actions visant à compromettre la confidentialité, l'intégrité ou la disponibilité d'une ressource. La notion d'intrusion est à considérer au sens large et comprend les notions d'anomalies et d'usage abusif des ressources.

D'un côté, il y a les systèmes de détection d'intrusions (IDS pour Intrusion Detection System) qui sont des mécanismes destinés à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Ils permettent ainsi d'avoir connaissance des tentatives réussies comme échouées des intrusions.

Dans le processus de détection d'intrusion manuelle, un analyste humain procède à l'examen de fichiers de logs (journaux) à la recherche de tout signe suspect pouvant indiquer une intrusion. Un système qui effectue une détection d'intrusion automatisée est appelé système de détection d'intrusion (IDS). Lorsqu'une intrusion est découverte par un IDS, les actions typiques qu'il peut entreprendre sont par exemple d'enregistrer l'information pertinente dans

un fichier ou une base de données, de générer une alerte par e-mail ou un message sur un pager ou un téléphone mobile. Déterminer quelle est réellement l'intrusion détectée et entreprendre certaines actions pour y mettre fin ou l'empêcher de se reproduire, ne font généralement pas partie du domaine de la détection d'intrusion. Cependant, quelques formes de réaction automatique peuvent être implémentées par l'interaction de l'IDS et de systèmes de contrôle d'accès comme les pare-feu. Le diagramme suivant illustre le fonctionnement d'un IDS.

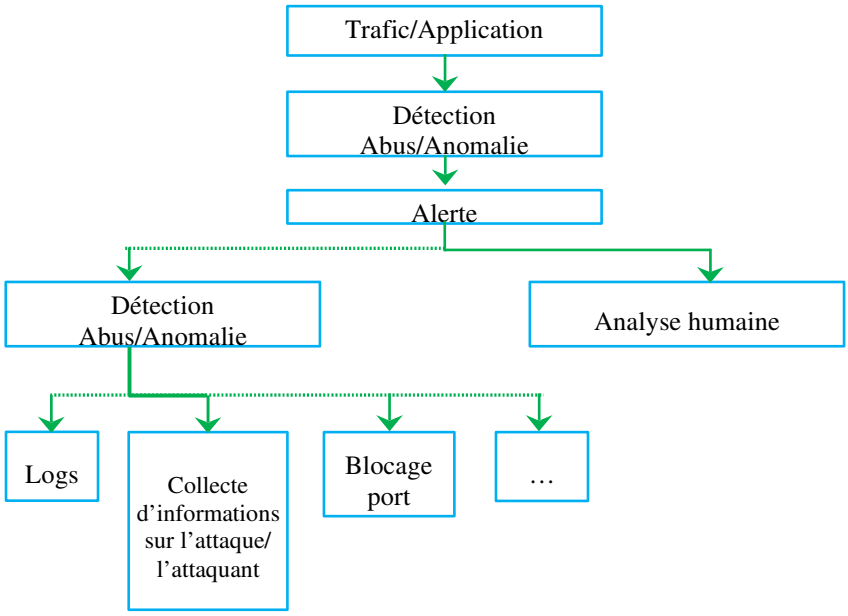


Figure 3-6 : Fonctionnement d'un IDS

D'un autre côté, il y a les systèmes de prévention d'intrusions (IPS pour Intrusion Prevention System) qui sont des mécanismes ayant pour but d'anticiper et de stopper les attaques. La prévention d'intrusion est appliquée par quelques IDS récents et diffère des techniques de détection d'intrusion décrites précédemment. Au lieu d'analyser les *logs* du trafic, c'est-à-dire découvrir les attaques après qu'elles se soient déroulées, la prévention d'intrusion essaie de prévenir ces attaques. Là où les systèmes de détection d'intrusion se contentent de donner l'alerte, les systèmes de prévention d'intrusion bloquent le trafic jugé dangereux.

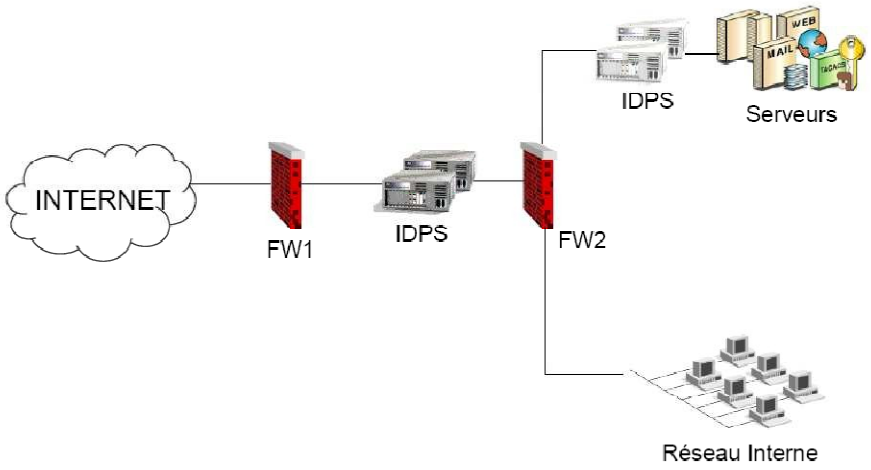


Figure 3-7 : Architecture d'un système de prévention d'intrusions réseau (NIPS) ou de détection d'intrusions (NIDS).

Le principe de fonctionnement d'un IPS est symétrique à celui d'un IDS (IDS hôte et IDS réseau), ajoutant à cela l'analyse des contextes de connexion, l'automatisation d'analyse des *logs* et la coupure des connexions suspectes.

Contrairement aux IDS classiques, aucune signature n'est utilisée pour détecter les attaques. Avant toute action, une décision en temps réel est exécutée (c'est-à-dire que l'activité est comparée à un ensemble de règles). Si l'action est conforme à l'ensemble de règles, la permission de l'exécuter sera accordée et l'action sera exécutée. Si l'action est illégale (c'est-à-dire que si le programme demande des données ou veut les changer alors que cette action ne lui est pas permise), une alarme est donnée. Dans la plupart des cas, les autres détecteurs du réseau (ou une console centrale) en seront aussi informés dans le but d'empêcher les autres ordinateurs d'ouvrir ou d'exécuter des fichiers spécifiques.

Plusieurs stratégies de prévention d'intrusion existent :

- Host-based memory and process protection : qui surveille l'exécution des processus et les tue dès lors qu'ils ont l'air dangereux (buffer overflow). Cette technologie est utilisée dans les KIPS (Kernel Intrusion Prevention System) ;
- Session interception (ou session sniping) : qui termine une session TCP avec la commande TCP Resest (« RST »). Ceci est beaucoup utilisé dans les NIPS (Network Intrusion Pevention System) ;
- Gateway intrusion detection : si un NIPS est placé en tant que routeur, il bloque le trafic ou envoie des messages aux autres routeurs du réseau pour modifier adéquatement leurs listes d'accès pour bloquer les sources jugées agressives.

Le diagramme ci-après illustre le fonctionnement d'un IPS :

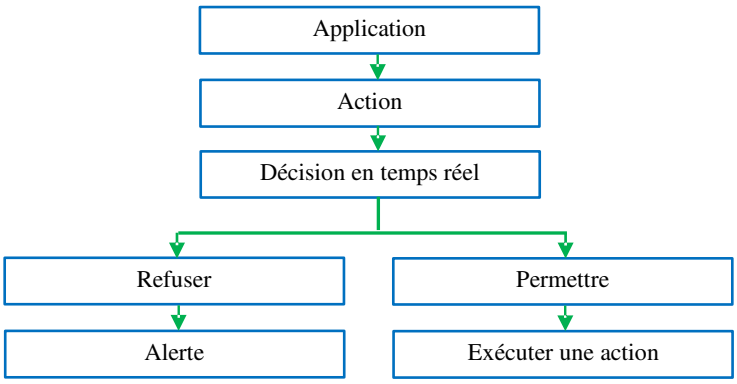


Figure 3-8 : Fonctionnement d'un IPS

III.2.2 Avantages des systèmes de protection contre les intrusions

En profitant des bugs logiciels, en exploitant les faiblesses des protocoles et en piratant les mots de passe, les pirates peuvent rechercher et exploiter des portes ouvertes dans les lignes de défense d'un réseau d'entreprise. Or ces portes peuvent être fermées par un système de détection ou de prévention d'intrusions :

- détection précise des attaques ;
- arrêt des attaques ;
- simplification de la gestion de la sécurité ;
- documentation appropriée (journaux détaillés) ;
- flexibilité requise pour respecter les règles de sécurité ;
- double vérification (après celle des pare-feux mal configurés) ;

- vérification de la bonne application des règles de sécurité ;
- interception des attaques que les pare-feu laissent passer de manière légitime ;
- interception des tentatives infructueuses ;
- interception des piratages venant de l'intérieur ;
- détection des attaques anormales lancées depuis un terminal inoccupé ;
- détection de failles pouvant être exploitées par des intrus ;
- documentation fournie avant, pendant et après une attaque.

Les systèmes de protection contre les intrusions peuvent être déployés au niveau des points d'accès, derrière les pare-feux, sur divers segments et serveurs ou à différents emplacements où ils feront office d'agents de sécurité du périmètre. En surveillant le trafic pour protéger les systèmes des attaques internes et externes sur le réseau, ces systèmes détectent et arrêtent les pirates qui tentent de s'introduire dans les réseaux. Les méthodes de détection incluent l'utilisation de signatures d'attaque, la vérification d'anomalies de protocoles et d'actions inhabituelles.

Les pirates exploitent constamment de nouvelles failles. En trouvant d'autres méthodes pour accéder à votre réseau interne, ils lancent de nouvelles attaques sophistiquées qui ne suivent pas un schéma défini. Tandis que la détection basée sur les signatures est un système robuste, la détection des anomalies de protocoles peut être utilisée pour identifier les diverses attaques qui n'observent pas les scénarii habituels.

Ainsi, un grand nombre d'attaques réseau peuvent être déjouées grâce aux systèmes de détection et de prévention des intrusions. Ce sont des outils qui demandent une configuration fine et une analyse régulière des fichiers journaux.

Les systèmes IDS et IPS appliquent des méthodes similaires lorsqu'ils essaient d'intercepter des intrus ou des attaques sur le réseau. Ils ont généralement une base de données de signatures, qui peut être régulièrement mise à jour à mesure que de nouvelles menaces sont identifiées.

Les administrateurs de sécurité déploient des agents ou des capteurs, logiciels ou matériels, en des points clés de leur réseau. Généralement en périphérie ou sur les passerelles vers d'autres réseaux en des endroits où le trafic réseau converge, et qui ont été identifiés comme étant des points de détection et d'interception stratégiques. Les placer derrière les pare-feux est toujours un bon choix. Les capteurs à distance envoient alors leurs rapports à une machine centrale qui gère les règles du système. Il stocke les données dans un seul endroit afin de faciliter l'enregistrement, les alertes et l'élaboration de comptes-rendus.

Les capteurs IDS/IPS déployés sur le réseau examinent les flux de données qui transitent à leur niveau, puis analysent le trafic et le comparent aux signatures contenues dans leurs bases de données. Lorsqu'une correspondance est trouvée, le système active et effectue les tâches définies par l'administrateur: interrompre la connexion TCP, alerter l'équipe de sécurité ou stocker les informations dans un journal ou log en vue d'une analyse ultérieure. Naturellement, les performances du réseau doivent être évaluées avant de déployer un capteur.

Il est également possible de déployer différents types de systèmes pour offrir au réseau plusieurs niveaux de sécurité. Par exemple, en combinant une solution matérielle (appliance) pour contrôler les points d'entrée/sortie du réseau avec des logiciels basés sur hôte pour surveiller les machines critiques.

III.3 Typologies et familles des systèmes de protection contre les intrusions

III.3.1 Typologies des systèmes de protection contre les intrusions

La caractérisation des différents systèmes de protection contre les intrusions permet de les différencier suivant un certain nombre de caractéristiques. Cette caractérisation a conduit à la classification terminologique présentée dans la figure suivante.

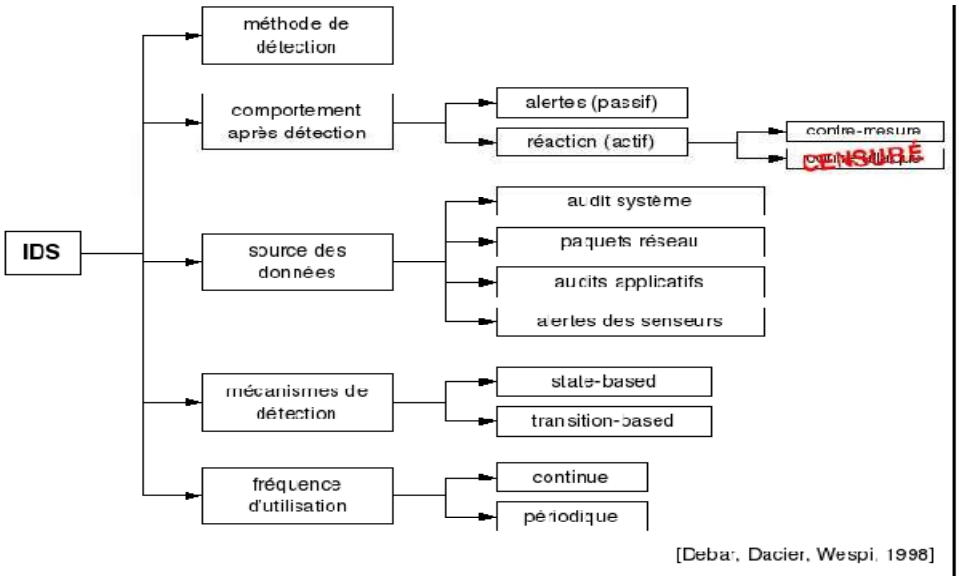


Figure 3-9 : Classification terminologique des systèmes de protection contre les intrusions

Dans un premier temps, on peut faire une distinction assez fondamentale sur la méthode de détection utilisée par les systèmes de protection contre les intrusions. Il existe deux grandes catégories de méthodes de détection:

celles basées sur une approche comportementale (par exemple l'analyse statistique, l'analyse bayésienne, les réseaux neuronaux)

et celles basées sur une approche par scénarii (par exemple la recherche de signatures ou le pattern matching).

Globalement, les approches comportementales visent à reconnaître un comportement anormal, que ce soit par rapport à une définition du comportement normal ou anormal fournie au système de détection d'intrusion (par exemple une spécification de protocole de communication) ou par rapport à une modélisation des comportements normaux ou anormaux apprise à partir d'une observation préalable du système (en salle blanche, ou tout simplement en réel). Dans le cadre d'une approche comportementale, l'apprentissage semble donc possible, tout comme la possibilité de détecter des attaques inconnues au moment de la conception de l'IDS, à condition qu'elles génèrent des anomalies perceptibles dans le fonctionnement normal.

Par contre, dans une approche par scénarii, les systèmes de protection contre les intrusions s'appuient sur une base de connaissance préexistante décrivant les comportements normaux ou anormaux et utilise cette connaissance pour la reconnaissance des évènements produits par des actions d'intrusions dans le système informatique qu'ils observent. Cette méthode

implique donc la constitution et la mise à jour régulière d'une base de connaissance référençant les différentes attaques connues susceptibles d'être mises en œuvre dans un système informatique. C'est à partir de ces informations, affinées par l'administrateur en fonction du système surveillé, que les systèmes de protection contre les intrusions identifient les éventuelles attaques ayant lieu dans les systèmes informatiques.

Dans cette approche, les systèmes de protection contre les intrusions se focalisent donc sur l'identification des utilisations abusives (misuse). Une autre mise en œuvre conforme à la terminologie mais originale dans la pratique de cette approche de détection par scénarii consiste à constituer une base de connaissance des comportements permis dans le système (et non des comportements abusifs) pour configurer les actions de détection (des utilisations normales en quelque sorte).

Dans un second temps, on peut aussi comparer les systèmes de protection contre les intrusions en fonction du mode de fonctionnement des mécanismes de détection qu'ils mettent en œuvre. De manière générale, un système de protection contre les intrusions peut tenter d'identifier des attaques en s'appuyant sur des informations relatives aux transitions ayant lieu dans le système (l'exécution de certains programmes, de certaines séquences d'instructions, l'arrivée de certains paquets réseau, etc.) ou bien en étudiant l'état de certaines parties du système (par exemple, l'intégrité des programmes stockés, les privilèges des utilisateurs, les transferts de droits, etc.).

III.3.2 Familles des systèmes de protection contre les intrusions

Selon l'endroit qu'ils surveillent et ce qu'ils contrôlent (les « sources d'information »), deux familles principales d'IDS sont usuellement distinguées:

III.3.2.1 Les IDS réseaux (NIDS) : Une solution plus courante

Imaginons qu'une requête malintentionnée ait passé le barrage du firewall : il faut donc l'arrêter. La méthode la plus classique consiste à faire appel à un Network IDS - une solution de détection d'intrusion largement éprouvée. Son rôle sera d'immobiliser chaque requête, de l'analyser et de lui laisser continuer son chemin seulement si elle ne correspond pas au portrait-robot d'une attaque référencée. Avant d'opter pour un tel système, il faut connaître les points clés de cette solution.

Le rôle essentiel d'un IDS réseau, appelé NIDS (Network-based Intrusion Detection System), est l'analyse et l'interprétation des paquets circulant sur ce réseau. Afin de repérer les paquets à contenu malicieux comme par exemple des expressions contenant « */etc/passwd* », des signatures sont créées. Des détecteurs (souvent de simples hôtes) sont utilisés pour analyser le trafic et si nécessaire envoyer une alerte. Un IDS réseau travaille sur les trames réseau à tous les niveaux (couches réseau, transport, application). De plus en plus, en disséquant les paquets et en « comprenant » les protocoles, il est capable de détecter des paquets malveillants conçus pour outrepasser un pare-feu aux règles de filtrage trop laxistes, et de chercher des signes d'attaque à différents endroits sur le réseau. Quelques exemples de NIDS : NetRanger, NFR, Snort, DTK, ISS RealSecure7.

Les IDS réseau ont des atouts, par exemple, les détecteurs peuvent être bien sécurisés puisqu'ils se « contentent » d'observer le trafic, les scans sont détectés plus facilement grâce aux signatures, etc. Cependant, les problèmes majeurs liés aux NIDS sont de conserver

toujours une bande passante suffisante pour l'écoute de l'ensemble des paquets, et de bien positionner l'IDS pour qu'il soit efficace.

Premier gage de qualité pour un Network IDS : l'exhaustivité du fichier contenant les signatures des attaques. Ce fichier est centralisé et mis à jour par le fabricant de solutions de Network IDS. Il faut donc penser très régulièrement à en télécharger la liste la plus récente. Par extension, la qualité des équipes de veille du fabricant conditionne largement l'efficacité de ses produits : les plus grandes marques emploient plusieurs dizaines de personnes à la mise à jour de cette liste de signatures.

Un des points cruciaux des NIDS concerne le choix de leurs emplacements. « Une sonde placée à un mauvais endroit peut être inefficace », soutient Philippe Solini, Network Design Consultant chez Unisys. Il est d'ailleurs courant que l'on ne puisse pas se contenter d'un seul système de filtrage : plus un réseau est complexe, plus il présente de vulnérabilités. Il en devient logiquement plus difficile à protéger. Mais chaque network IDS rajouté coûte cher : ces machines sont particulièrement gourmandes en ressources. "Les débits analysés sont très lourds, il est donc nécessaire de dédier au Network IDS des machines très puissantes, ou des appliances (boites noires) spécialisés pour parvenir à les soutenir", explique Philippe Solini.

III.3.2.2 Le Host IDS : Une solution qui monte

En somme, le Network IDS est un gendarme qui compare chaque trame à une banque de portraits robots. Mais il ne garantit pas à lui seul un niveau de sécurité proche de 100 %. Pour y parvenir, il faut mettre en faction un autre gendarme, qui observera le comportement de chaque trame et signalera tout ce qui lui paraîtra inhabituel. C'est le rôle du Host IDS, une véritable sonde qui est placée individuellement sur chaque système à protéger. Un système qui corrige les faiblesses des Network IDS.

La technologie Host IDS excelle dans la détection des anomalies connues et inconnues : si une attaque parvient à se faufiler à travers les mailles du filet, la sonde va la repérer : "Le Host IDS réalise une photographie du système à un moment donné. Il définit tout ce qui est légitime. Tout ce qui sort du cadre et des habitudes du système est considéré comme une attaque. Une modification de la base de registres sera donc bloquée et fera l'objet d'une alerte", explique Pascal Delprat (Consultant en sécurité chez Cisco en France). Un travail complémentaire à celui du Network IDS.

Une sonde Host IDS est moins onéreuse qu'un Network IDS, mais on doit en placer une sur chaque machine à surveiller. On les réserve donc le plus souvent aux machines très protégées. Elles sont également beaucoup moins gourmandes en ressources systèmes qu'un Network IDS: on les trouve donc sous forme de logiciel, et non plus intégrées à un serveur ou une appliance comme les Network IDS. Placées sur une machine, elles ne consomment en effet pas plus de 5 % des ressources.

Ensemble, les deux gendarmes font accéder un réseau d'entreprise à un niveau de protection optimal. A condition d'être chapeautés par un brigadier-chef : ils ne savent pas travailler correctement sans être encadrés. Le problème de l'administration des IDS au quotidien représente en effet le point le plus délicat et le plus crucial pour un système de détection d'intrusion. Si on le néglige, il est préférable de garder son budget pour l'investir ailleurs.

Les systèmes de détection d'intrusion basés sur l'hôte (poste de travail, serveur, etc.), ou HIDS (Host-based IDS), analysent exclusivement l'information concernant cet hôte. Comme ils n'ont pas à contrôler le trafic du réseau mais "seulement" les activités d'un hôte, ils se montrent habituellement plus précis sur les variétés d'attaques. Ces IDS utilisent deux types

de sources pour fournir une information sur l'activité : les logs et les traces d'audit du système d'exploitation. Chacun a ses avantages : les traces d'audit sont plus précises, détaillées et fournissent une meilleure information ; les logs, qui ne fournissent que l'information essentielle, sont plus petits et peuvent être mieux analysés en raison de leur taille. Il n'existe pas de solution unique HIDS couvrant l'ensemble des besoins, mais les solutions existantes couvrent chacune un champ d'activité spécifique, comme l'analyse de logs système et applicatifs, la vérification de l'intégrité des systèmes de fichiers, l'analyse du trafic réseau en direction/provenance de l'hôte, le contrôle d'accès aux appels système, l'activité sur les ports réseau, etc. Par exemple, le démon syslog peut être considéré partiellement comme un système HIDS, car il permet de consigner certaines activités, et à l'aide d'un analyseur comme Swatch, de détecter certaines tentatives d'intrusion (comme bad login) ; Tripwire, centrant son activité sur l'intégrité du système de fichiers, peut aussi être vu comme un HIDS, Security Manager, etc.

Les systèmes de détection d'intrusion basés sur l'hôte ont certains avantages : l'impact d'une attaque peut être constaté et permet une meilleure réaction, des attaques dans un trafic chiffré peuvent être détectées (impossible avec un IDS réseau), les activités sur l'hôte peuvent être observées avec précision, etc. Ils présentent néanmoins des inconvénients, parmi lesquels : les scans sont détectés avec moins de facilité ; ils sont plus vulnérables aux attaques de type DoS ; l'analyse des traces d'audit du système est très contraignante en raison de la taille de ces dernières ; ils consomment beaucoup de ressources CPU, etc.

Une version d'IDS hybride est possible et désormais supportée par différentes offres commerciales. Même si la distinction entre HIDS et NIDS est encore courante, certains HIDS possèdent maintenant les fonctionnalités de base des NIDS. Des IDS bien connus comme ISS RealSecure se nomment aujourd'hui "IDS hôte et réseau". Dans un futur proche, la différence entre les deux familles devrait s'estomper de plus en plus (ces systèmes devraient évoluer ensemble). De ces deux familles principales, de nombreuses variantes sont issues et peuvent être étudiées en profondeur en consultant les rapports de recherche concernant la détection et la prévention d'intrusion de Nathalie Dagorn (lien à retrouver)

Concrètement, ce sont donc les systèmes de détection d'intrusion réseau utilisant des bases de signatures qui dominent les mises en œuvre opérationnelles disponibles sur le marché.

III.4 Limites des systèmes de protection contre les intrusions

La plupart des reproches faits aux systèmes de protection contre les intrusions concerne en réalité les systèmes de détection d'intrusion. C'est pourquoi les systèmes de prévention d'intrusions sont souvent considérés comme les améliorations des IDS.

Les systèmes de protection contre les intrusions doivent pouvoir supporter le trafic maximal attendu à l'endroit où ils seront placés. Si un capteur ne peut pas gérer le débit, des paquets de données seront perdus, et les données transitant par ce point ne seront pas toutes analysées. Cette situation peut même avoir un impact sur les performances globales du réseau en créant un goulet d'étranglement. Il est donc préférable de surestimer le trafic réseau potentiel transitant par le point de déploiement du capteur que le contraire.

La plus grande menace qui pèse sur les déploiements d'IDS/IPS est que, au fil du temps, l'équipe de sécurité ne fasse plus attention aux données enregistrées. C'est un point qu'il faut prendre en compte lors du choix des règles de sécurité. Même si un grand nombre de

messages sont interceptés à tort lorsqu'un système est déployé la première fois, celui-ci doit être constamment reconfiguré pour en réduire peu à peu le nombre. Le but étant de disposer d'un système robuste et pratique susceptible un jour de sauver les données de l'entreprise.

L'une des principales limites qu'on connaît aux IDS est le phénomène des faux positifs et des faux négatifs. Après le phénomène de faux positifs et des faux négatifs, il existe encore plusieurs autres imperfections et limites souvent attribuées aux IDS. Il s'agit entre autres du mode promiscuité, de la définition et maintenance des signatures, leur apprentissage et leur configuration de l'IDS et enfin les limites générales.

III.4.1 Faux positifs et faux négatifs

Parmi les comportements possibles pour un IDS, on peut envisager les quatre possibilités recensées dans le tableau suivant qu'une intrusion soit ou non en cours dans le système informatique et que le système de détection d'intrusion ait émis ou non une alerte.

	Pas d'alerte	Alerte
Pas d'attaque	Vrai négatif	Faux négatif
Attaque en cours	Faux négatif	Vrai négatif

Tableau 3-2 : Comportements envisageables pour un IDS

Parmi ces quatre comportements, les vrais négatifs et les vrais positifs correspondent aux comportements souhaités. Toutefois un IDS est généralement imparfait et conduit à l'apparition des deux autres comportements non désirés. Parmi eux, un faux négatif correspond à une attaque non détectée, et un faux positif à l'émission d'une fausse alerte. Les différents IDS souffrent généralement d'imperfections donnant lieu à l'apparition de ces comportements non désirés, mais selon des axes différents suivant les méthodes de détection qu'ils utilisent.

Un reproche fréquemment fait en direction des IDS utilisant une méthode de détection comportementale est de contenir dans leur principe même de fonctionnement la possibilité de fausses alertes (un changement de comportement légitime détecté comme anormal) ou de faux négatifs (par exemple pour une attaque très lente) ; tandis que les approches par scénarii semblent théoriquement être plus exactes. Toutefois, la base de connaissance utilisée dans les IDS par scénarii exige une maintenance constante et, dans la pratique, souffre également nécessairement d'imperfections.

Bien que les faux négatifs soient effectivement le premier des comportements indésirables pour un IDS, les faux positifs sont importants aussi : ils peuvent conduire à une réelle perte de confiance dans les capacités de détection de l'IDS de la part des administrateurs qui peut finir par remettre en cause la finalité de l'IDS. C'est même une des voies d'attaque envisageables contre un système équipé d'un IDS : générer un nombre suffisamment important de fausses alertes pour réduire l'attention des administrateurs et dissimuler une attaque réelle. De plus, dans la pratique, les faux positifs dus à l'environnement de l'IDS ou à des signatures d'attaque un peu trop affirmatives sont souvent nombreux ; et ceci nécessite généralement un reparamétrage de l'IDS pour faciliter son exploitation, au prix de l'introduction de possibilités de faux négatifs. La gestion des faux positifs est le premier problème auxquels sont confrontés les administrateurs d'un IDS, et il est généralement de taille.

Les IDS basés sur une approche par scénarii, c'est à dire la plupart des IDS courants, souffrent sur ce point d'un réel problème qui demanderait certainement de développer à la fois les

possibilités d'adaptation de l'IDS à son environnement (peut-être par des moyens de corrélation) et une meilleure validation des signatures d'attaque disponibles.

L'utilisation de techniques de corrélation d'alertes provenant de plusieurs IDS semble être une des voies envisageables pour traiter ces problèmes d'analyse des alertes et notamment des fausses alertes. Dans ce cadre, la diversification des méthodes de détection utilisées par les différents IDS, ainsi que de leurs sources de données est aussi à nouveau envisageable. (Dans un certain sens, il s'agit d'ailleurs de ré-inventer la roue une fois de plus puisque le précurseur des systèmes de détection d'intrusion, nommé IDES, combinait déjà l'utilisation d'une approche comportementale -statistique- et d'une approche à base de règles -système expert-, dans les années 1980 du côté de Stanford.).

III.4.2 Le mode ‘‘promiscuous’’

L’utilisation du mode “promiscuous” présente quelques inconvénients, notamment :

- Réponse involontaire du système : par nature, les IDS doivent mettre leur carte réseau en mode “promiscuous” afin de pouvoir recevoir l'intégralité des trames circulant sur le réseau. Ainsi, l'IDS ne générera généralement aucun trafic et se contentera d'aspirer tous les paquets. Cependant, ce mode spécial désactive la couche 2 “liaison” de la machine (le filtrage sur les adresses MAC n'est plus activé). Il se peut alors que la machine réponde à certains messages (ICMP echo request généré avec l'outil Nemesis) ;
- Mise en évidence de la présence d’un IDS : le mode “promiscuous” génère des accès mémoire et processeur importants ; il est possible de détecter de telles sondes en comparant les latences de temps de réponse avec celles des machines du même brin LAN (ou proche). Des temps de réponse trop importants sont significatifs d'une activité gourmande en ressources telle que le sniffing, validant possiblement la présence d'un IDS ;
- L’utilisation du mode “promiscuous” implique d’installer une sonde par réseau commuté.

III.4.3 La définition et la maintenance des signatures

Toutes les attaques ne sont pas détectées, selon les fonctionnalités du système, la définition de la signature, la mise à jour de la base, la charge du système, etc. :

- Limites “humaines” : signatures pas à jour ou mal conçues. La détection d’abus a pour impératifs une bonne conception des signatures d’attaques et une mise à jour continue de la liste des signatures ;
- Contexte d’utilisation : parfois la technologie est basée sur des signatures qui ne reposent pas sur le contexte d’utilisation. La conséquence est double : de nombreux faux positifs et une dégradation importante des performances du système ;
- Même si la méthode des signatures de corps (y compris les signatures de chaîne) semble être assez sûre, il y a moyen de les contourner ;
- Vulnérabilité aux mutations : de par son manque de flexibilité, la détection par signatures d'attaques est très vulnérable aux mutations. D’une part, pour pouvoir définir une signature, il faut avoir déjà été confronté à l'attaque considérée ;

D'autre part, certaines de ces signatures se basent sur des caractéristiques “volatiles” d'un outil, comme par exemple le port qu'un cheval de Troie ouvre par défaut ou la valeur d’ISN (*Initial Sequence Number*) choisie par certains outils de piratage. Or ces logiciels sont souvent soit hautement configurables, soit *open source* donc librement modifiables. Les caractéristiques retenues pour définir la signature sont donc fragiles, et les signatures extrêmement sensibles aux mutations.

- Faute de définition, les *nouvelles attaques* passent l’IDS sans être détectées.

III.4.4 L’apprentissage et la configuration des IDS

L’apprentissage du comportement « normal » n’est pas aisé. Automatiser le raisonnement conduisant à penser que le comportement est “déviant” par rapport à celui connu est une tâche difficile. Par contre, cette technique est appliquée par défaut (la plupart du temps) par les administrateurs réseau ou système : lorsque quelque-chose paraît inhabituel (par exemple, des pics de bande passante, des services qui tombent, des systèmes de fichiers qui se remplissent plus vite qu’à l’accoutumée, etc.), l’usage veut que des recherches plus poussées soient entreprises.

Par ailleurs, toute anomalie ne correspond pas forcément à une attaque, cela peut être un changement de comportement de l’utilisateur ou un changement de la configuration du réseau. En règle générale, la convergence vers un modèle comportemental “normal” est plutôt longue.

Lors du paramétrage de l’IDS, toute la difficulté pour une détection efficace réside dans le choix des métriques, des modèles de comportement et dans la définition des différents profils. Pour toutes ces raisons, les IDS fonctionnant par détection d’anomalie sont reconnus comme étant très longs et fastidieux à configurer.

Même après une configuration efficace, rien n'empêche un pirate se sachant surveillé de “rééduquer” un tel système en faisant évoluer progressivement son modèle de convergence vers un comportement anormal pour l'analyste, mais tout-à-fait “normal” d'un point de vue statistique.

III.5 Etudes comparatives de quelques systèmes de protection contre les intrusions

Dans cette partie, nous allons effectuer une comparaison de quelques IDS et IPS. Il s’agit de les comparer suivant les critères comme l’analyse du trafic en temps réel, la capacité de blocage des attaques, les alertes en temps réel, la mise en log des paquets de données, les méthodes de filtrage. En analysant le tableau de comparaison suivant, on constate que tous les systèmes étudiés disposent des qualités suivantes :

L’analyse en temps réel ;
La détection des virus, des vers et des chevaux de troie ;
La détection des attaques internes et externes ;
La capacité de blocage des attaques ;
La détection des sondes externes et internes ;
La capacité de blocage des sondes.

Parmi ces systèmes, seuls Juniper IDP et Snort 2.1.3 peuvent s’exécuter dans les environnements Linux. Les autres pour la plupart fonctionnent dans les systèmes

d'exploitation Windows. Quant à SonicWALL IPS Service, il peut s'exécuter dans tous les environnements IP.

PRODUITS	CA eTRUST Intrusion detection 3.0	Juniper IDP	McAfee Intrushield série I	McAfee Intercept 5.0	Snort 2.1.3	SonicWALL IPS service
Fournisseur	Computer Associates	Juniper	McAfee	McAfee	Snort	ACA Pacific
Analyse du trafic en temps réel	Oui	Oui	Oui	Oui	Oui	Oui
Détection des virus/vers/chevaux de Troie	Oui	Oui	Oui	Oui	Oui	Oui
Détection des attaques externes	Oui	Oui	Oui	Oui	Oui	Oui
Détection des attaques internes	Oui	Oui	Oui	Oui	Oui	Oui
Capacité de blocage des attaques	Oui	Oui	Oui	Oui	Oui	Oui
Détection des sondes externes	Oui	Oui	Oui	Oui	Oui	Oui
Détection des sondes internes	Oui	Oui	Oui	Oui	Oui	Oui
Capacité de blocage des sondes	Oui	Oui	Oui	Oui	Oui	Oui
Définitions du blocage des sondes	Oui	Signatures avec données d'état, anomalie de protocole, détection des portes dérobées, anomalie de trafic, protection de couche 2, inondation Syn, profilage de la sécurité d'entreprise	Mise à jour, listes de blocage définies par l'utilisateur et règles personnalisables	Mise à jour, listes de blocage définies par l'utilisateur et règles personnalisables	Mise à jour, intégration tierce, personnalisables par l'utilisateur	Mises à jour
Alerte en temps réel	Courrier électronique, pager, application d'exécution, SNMP, console	Courrier électronique, syslog, SNMP, fichier journal, SMS externe	Console, courrier électronique, pager, SMS par courrier électronique	Console, courrier électronique, pager, SNMP, génération de processus	Fichiers journaux, courrier électronique, console, applications tierces	Fichiers journaux, courrier électronique, syslog, SGMS
Mise en logs des paquets de données	Espace de travail (propriétaire), base de données ODBC	Syslog, base de données internes	Oracles, MySQL	Microsoft SQL Server	ND	ND
Recherche de contenu	Oui	Oui	ND	ND	Oui	Oui
Mise en correspondance du contenu	Oui	Oui	ND	ND	Oui	Oui
Filtrage du contenu	Oui	Oui	ND	ND	Oui	Oui

Méthode de filtrage	Base de données d'URL	Définies par l'administrateur	ND	ND	Définies par l'administrateur	Liste noire, tierces, définies par l'administrateur
Outils de rapports	Oui	Oui	Oui	Oui	ND (vendus séparément)	ND (vendus séparément)
Système d'exploitation compatible	Windows 2000 (autonome), Windows 2000/2003/XP pour le moteur à distance	Console de gestion, Windows, Linux ; Serveur de gestion Linux, Solaris	Console de gestion Windows 2000	Système de gestion Windows 2000 ; console Windows NT, 2000, XP, agents Windows, Solaris, HP/UX	Linux, Windows	Tout environnement IP

Tableau 3-3 : Tableau comparatif de quelques systèmes de protection contre les intrusions

En ce qui concerne les alertes en temps réel, tous ces systèmes en sont dotés diversement. On a des alertes par SMS, par courrier électronique, sur les consoles, par le démon SYSLOG, les pagers etc.

Snort 2.1.3 et SonicWALL IPS ne font pas la mise en log des paquets de données. Cependant dans ce domaine le meilleur système est le McAfee Intrushield serie I car il peut travailler en interaction avec deux des meilleurs SGBD qui existent. Il s'agit de MySQL et Oracle.

III.6 Présentation de Snort, SnortSAM et de BASE

III.6.1 Description

Snort est un NIDS / NIPS provenant du monde Open Source. C'est pourquoi nous le recommandons fortement aux entreprises et organisations africaines en général car ces dernières n'ont pas souvent suffisamment de ressources financières à accorder à l'achat des logiciels propriétaires.

Avec plus de 2 millions de téléchargements, il s'est imposé comme le système de détection d'intrusions le plus utilisé. Sa version commerciale, plus complète en fonctions de monitoring, lui a donné bonne réputation auprès des entreprises.

Snort est capable d'effectuer une analyse du trafic réseau en temps réel et est doté de différentes technologies de détection d'intrusions telles que l'analyse protocolaire et le pattern matching. Snort peut détecter de nombreux types d'attaques : buffer overflows, scans de ports furtifs, attaques CGI, sondes SMB, tentatives de fingerprinting de système d'exploitation etc.

Snort est doté d'un langage de règles permettant de décrire le trafic qui doit être accepté ou collecté. De plus, son moteur de détection utilise une architecture modulaire de plugins.

Notons que Snort dispose de trois modes de fonctionnement : sniffer de paquets, logger de paquets et système de détection/prévention d'intrusions. Nous ne nous intéresserons qu'à ce dernier mode.

III.6.2 Installation

Pour installer Snort, deux méthodes sont possibles :

La première méthode est celle de l'installation automatique et qui consiste sur un système d'exploitation telle que Linux Debian Etch par exemple à exécuter tout simplement la commande suivante **:#apt-get install snort.** Il faut noter qu'avec l'installation automatique toutes les bibliothèques et autres logiciels nécessaires sont aussi automatiquement proposés et installés par le système.

La deuxième méthode consiste à télécharger les sources et de les compiler soi même avec les options et les bibliothèques que l'on désire.

Voici brièvement en quelques étapes comment on peut réaliser l'installation par la deuxième méthode.

1. Télécharger les sources sur www.snort.org. Lors de l'écriture de ce document, la dernière version stable était la 2.4.4.
2. Télécharger et installer les bibliothèques nécessaires pour Snort :
   - libpcap (http://www.tcpdump.org) : offre des fonctions de sniffer
   - PCRE (http://www.pcre.org) : permet d'utiliser des expressions régulières de type Perl. La compilation de ces bibliothèques se fait très aisément : **./configure, make, make install**.
3. Ouvrir un terminal, décompresser ensuite l'archive de Snort et se placer dans le répertoire des sources décompressées.
4. Configurer la compilation de Snort afin d'activer plusieurs fonctionnalités : ./configure [options].

   Deux options nous ont semblé intéressantes :

   - --with-mysql=DIR : activer le support de MySQL. Ainsi Snort enregistrera les alertes dans une base de données accessible par d'autres applications (ex : BASE, décrite plus loin). MySQL n'est bien sûr pas l'unique SGBD supporté. PostgreSQL ou Oracle peuvent également être utilisés avec les options – withpostgresql et --with-oracle.
   - --enable-flexresp : activer les réponses flexibles en cas de tentatives de connexion hostile. Pour activer cette option, la bibliothèque libnet (http://www.packetfactory.net/libnet) est nécessaire.
5. Compiler les sources : make
6. Installer Snort : make install en mode root
7. Pour que Snort puisse fonctionner en mode détection/prévention d'intrusions, il est nécessaire de lui fournir des fichiers de règles. Le site de Snort propose deux types de règles : les règles officielles et les règles créées par la communauté. Certaines règles officielles ne sont disponibles que pour les utilisateurs enregistrés, tandis que les règles communautaires sont disponibles à tous et mises à jour régulièrement. Il est cependant important de noter que les règles proposées par la communauté n'ont pas été forcément testées par l'équipe officielle de Snort. Après téléchargement, l'archive des règles doit être décompressée. Il est conseillé de placer le répertoire rules dans le dossier de Snort. Nous pouvons remarquer que les règles consistent en de simples fichiers textes, et qu'un fichier un peu spécial est présent : **snort.conf**. Ce dernier va nous permettre de configurer Snort.

III.6.3 Configuration

Afin de configurer correctement Snort pour qu'il puisse fonctionner en mode détection d'intrusions, il faut modifier le fichier **snort.conf**. L'emplacement par défaut de ce fichier doit normalement être /etc/snort.conf. Cependant, il sera possible de spécifier un autre emplacement lors de l'exécution de Snort, à l'aide de l'option -c.

Le fichier de configuration contient de nombreuses options paramétrables, ainsi que des explications pour pouvoir les modifier correctement. Nous n'allons nous intéresser ici qu'à quelques variables :

- La variable HOME_NET permet de spécifier quels réseaux ou quelles interfaces seront surveillées par Snort. La valeur any signale à Snort de surveiller tout le trafic.
- Si le réseau à surveiller possède des serveurs DNS, SMTP, FTP, etc , il est possible de spécifier les adresses IP de ces serveurs via les variables DNS_SERVERS, SMTP_SERVERS, ... Si le réseau ne possède pas un type spécifique de serveur, il est conseillé de commenter (avec le caractère #) la ligne concernée, afin d'optimiser le traitement de Snort. En effet, il est inutile d'analyser du trafic HTTP si aucun serveur Web n'est disponible.
- Certains ports de services peuvent être configurés via des variables telles que HTTP_PORTS ou ORACLE_PORTS.
- La variable RULE_PATH est très importante. Elle permet de spécifier le répertoire où sont stockés les fichiers de règles de Snort.
- Les directives include permettent d'inclure des fichiers de règles. Ici encore, il est conseillé de n'inclure que les règles nécessaires en fonction des services disponibles sur le réseau.

III.6.5 Exécution

L'exécution de Snort se fait en lançant l'exécutable snort en mode root et avec différentes options. Voyons les principaux arguments de Snort :

- -A : générer des alertes. Activé par défaut avec l'option –c
- -c <emplacement de snort.conf> : lancer Snort avec des fichiers de règles.
- -l <répertoire de log> : spécifier le répertoire où les logs d'alertes seront stockés (défaut : /var/log/snort)
- -v : mode verbose. Permet d'afficher les paquets capturés
- -T : mode test. Permet de tester la configuration de Snort

Avant de lancer Snort en mode NIDS, il est préférable de tester si le programme arrive à récupérer les paquets qui circulent sur le réseau. Pour cela, nous pouvons par exemple lancer

Snort en simple mode Sniffer : snort -v. Si aucun paquet n'est capturé et affiché, il est probable que Snort n'écoute pas sur la bonne interface. L'option -i permet de spécifier une autre interface.

Lançons maintenant Snort en mode NIDS. Pour cela, nous lui précisons l'emplacement du fichier de configuration avec l'option –c : **#snort -c /opt/snort/rules/snort.conf**

Toutes les alertes détectées sont ainsi stockées dans le fichier « /var/log/snort/alert ». Pour chaque alerte, Snort donne une priorité, une description, les flags des paquets et éventuellement des adresses sur Internet où se trouvent de plus amples informations sur la tentative d'intrusion.

Exemple :

[**] [1:1384:8] MISC UPnP malformed advertisement [**]
[Classification: Misc Attack] [Priority: 2]
03/25-17:34:49.251861 192.168.0.1:1900 ->
239.255.255.250:1900
UDP TTL:1 TOS:0x0 ID:37277 IpLen:20 DgmLen:437
Len: 409
[Xref =>
http://www.microsoft.com/technet/security/bulletin/MS01-
059.mspx][Xref => http://cve.mitre.org/cgibin/
cvename.cgi?name=2001-0877][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-
0876][Xref => http://www.securityfocus.com/bid/3723]

III.6.6 Création de nouvelles règles

Bien que le site officiel de Snort propose des règles prêtes à l'emploi et régulièrement mises à jour, il peut être intéressant de créer ses propres règles afin d'adapter au mieux Snort au réseau qu'il doit surveiller et protéger. Par convention, les nouvelles règles personnelles sont à placer dans le fichier local.rules.

Une règle Snort est composée de deux parties et possède le format suivant : Header (Options).

Le format de la partie Header est défini de la manière suivante : action protocole adresse1 port1 direction adresse2 port2

Le champ action peut prendre les valeurs suivantes :

- alert : générer une alerte + logger le paquet
- log : logger le paquet
- pass : ignorer le paquet
- activate : activer une règle dynamique
- dynamic : définir une règle dynamique, qui est passive tant qu'elle n'est pas activée par une autre règle
- drop : demander à iptables (Netfilter) de bloquer le paquet, puis le logger
- reject : demander à iptables de bloquer le paquet, puis le logger, et envoyer une commande TCP RST (reset) ou une réponse ICMP Host unreachable
- sdrop : demander à iptables de bloquer le paquet. Ce dernier n'est pas loggé.

Le champ protocole spécifie le protocole pour lequel la règle s'applique. Les valeurs possibles sont : tcp, udp, icmp ou ip.

Les champs adresse1 et adresse2 indiquent l'adresse IP source et destination du paquet. Le mot clé any permet de spécifier une adresse quelconque. Les adresses doivent être numériques, les adresses symboliques ne sont pas acceptées.

Les champs port1 / port2 spécifient les numéros de port utilisés par la source et la destination. Le mot clé any permet de spécifier un port quelconque. Des noms de services peuvent être utilisés : tcp, telnet, ... De même des plages de ports peuvent être spécifiées avec le caractère « **: ».**

Le champ direction spécifie l'orientation du paquet. Cet opérateur peut prendre deux valeurs :
►: adresse1 vers adresse2
◄►:de adresse1 vers adresse2, ou de adresse2 à adresse1
Notons qu'il n'y a pas d'opérateur ◄.
La partie Options des règles contient différentes options, séparées par un point-virgule, qui vont permettre de préciser des critères de détection. Pour chaque option, le format est nomOption : valeur1 [, valeur2, ...]

Voici les options importantes :

- msg : spécifier le message qui sera affiché dans le log et dans l'alerte
- reference : faire référence à un site expliquant l'attaque détectée
- classtype : définir la classe de l'attaque (troyen, shellcode, ...)
- priority : définir la sévérité de l'attaque
- content : spécifier une chaîne de caractères qui doit être présente dans le paquet pour déclencher l'action de la règle
- rawbytes : spécifier une suite d'octets qui doit être présente dans le paquet pour déclencher l'action de la règle
- uricontent : identique à content mais est adapté au format normalisé des URI (ex : hexadécimal accepté)
- pcre : utiliser une expression régulière compatible Perl pour spécifier le contenu du paquet
- ttl : spécifier la valeur du TTL du paquet
- flags : spécifier la présence d'un flag TCP dans le paquet (ex : SYN, FIN, ...)
- fragbits : vérifier la présence de certains bits IP (more fragments, don't fragment ou bit réservé)
- session : extraire toutes les informations de la session TCP à laquelle le paquet suspect appartient
- resp : activer une réponse flexible (flexresp) afin de bloquer l'attaque. Il est ainsi possible d'envoyer une commande TCP ou ICMP précise. Cette option nécessite l'activation du mode flexresp lors de la compilation de Snort.
- limit : limiter le nombre d'actions pendant un intervalle de temps pour le même événement.

Exemple de règle :

alert tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEBATTACKS /bin/ls command attempt"; uricontent:"/bin/ls"; nocase; classtype:web-application-attack;)

Cette règle permet de générer une alerte quand un paquet provient d'un couple (adresse:port) quelconque, est à destination des serveurs HTTP définis dans snort.conf, et contient la chaîne « /bin/ls » dans l'URI. Le message de l'alerte sera « WEB-ATTACKS /bin/ls command

attempt ». Cette attaque sera classée dans la classe web-application-attack (priorité medium par défaut).
Il est bien sûr impossible d'être exhaustif ici pour décrire le format des règles Snort. Le manuel utilisateur disponible sur le site officiel indique comment utiliser aux mieux le langage des signatures de Snort.

III.6.7 SnortSam

SnortSam est un plugin Open-Source et multi-plateforme pour Snort. Il permet de bloquer automatiquement des adresses IP lorsqu'il détecte une tentative d'intrusion. Le blocage se fait en communiquant avec un firewall matériel (ex : Cisco Pix) ou logiciel (ex: PacketFilter, IPtables etc).

SnortSam est construit autour d'une architecture client / serveur (Snort / SnortSam) permettant de mettre en place le NIPS de manière distribuée. De plus, pour des raisons de sécurité, toutes les communications réalisées entre Snort et l'agent de SnortSam sont cryptées à l'aide de l'algorithme TwoFish.

Parmi les fonctionnalités intéressantes, on notera la présence d'une « White-List », c'est-à-dire une liste d'adresses IP qui ne peuvent pas être bloquées. Cela représente une sécurité pour éviter un blocage d'adresses sensibles (routeur, serveur Intranet etc) en cas de spoofing de la part du pirate.

Le plugin SnortSam est également doté d'un système de log et de notification par email des événements.

La mise en place d'actions de blocage est très simple. Il suffit de modifier les règles Snort pour signaler que la détection de certaines signatures doit provoquer un blocage. Pour cela, le mot clé fwsam a été rajouté. Il permet notamment de spécifier une durée de blocage. Cette option de durée peut-être intéressante lors d'un blocage après des tentatives répétées d'authentification avec un mot de passe erroné.

III.6.8 La console BASE

Par défaut, les alertes de Snort sont enregistrées dans un simple fichier texte. L'analyse de ce fichier n'est pas aisée, même en utilisant des outils de filtre et de tri. C'est pour cette raison qu'il est vivement conseillé d'utiliser des outils de monitoring. Parmi ceux-ci, le plus en vogue actuellement est BASE (Basic Analysis and Security Engine), un projet open-source basé sur ACID (Analysis Console for Intrusion Databases). La console BASE est une application Web écrite en PHP qui interface la base de données dans laquelle Snort stocke ses alertes.
Pour fonctionner, BASE a besoin d'un certain nombre de dépendances :

- Un SGBD installé, par exemple MySQL
- Snort compilé avec le support de ce SGBD
- Un serveur HTTP, par exemple Apache
- L'interpréteur PHP avec les supports pour le SGBD choisi, la bibliothèque GD et les sockets.
- La bibliothèque ADODB : http://adodb.sourceforge.net

Nous ne détaillerons pas ici l'installation de chaque dépendance. La documentation livrée avec les sources de BASE (disponibles sur http://secureideas.sourceforge.net) fournit les informations nécessaires.

Notons cependant que l'archive des sources de Snort dispose également d'un dossier *schemas* contenant le code SQL pour créer la structure de la base de données pour différents SGBD. Le fichier *doc/README.database* donne toutes les indications pour créer le schéma de la base de données.
Afin que Snort enregistre les alertes dans la base de données, il ne faut pas oublier de modifier le fichier snort.conf et rajouter une ligne output database avec les informations pour se connecter à la base de données.
Exemple : output database: log, mysql, user=snortusr password=pwd dbname=snort host=localhost

Après configuration et installation de BASE ainsi que de toutes ses dépendances, nous pouvons y accéder avec un navigateur internet. Si tout se passe bien, un écran similaire à l'illustration suivante est obtenu :

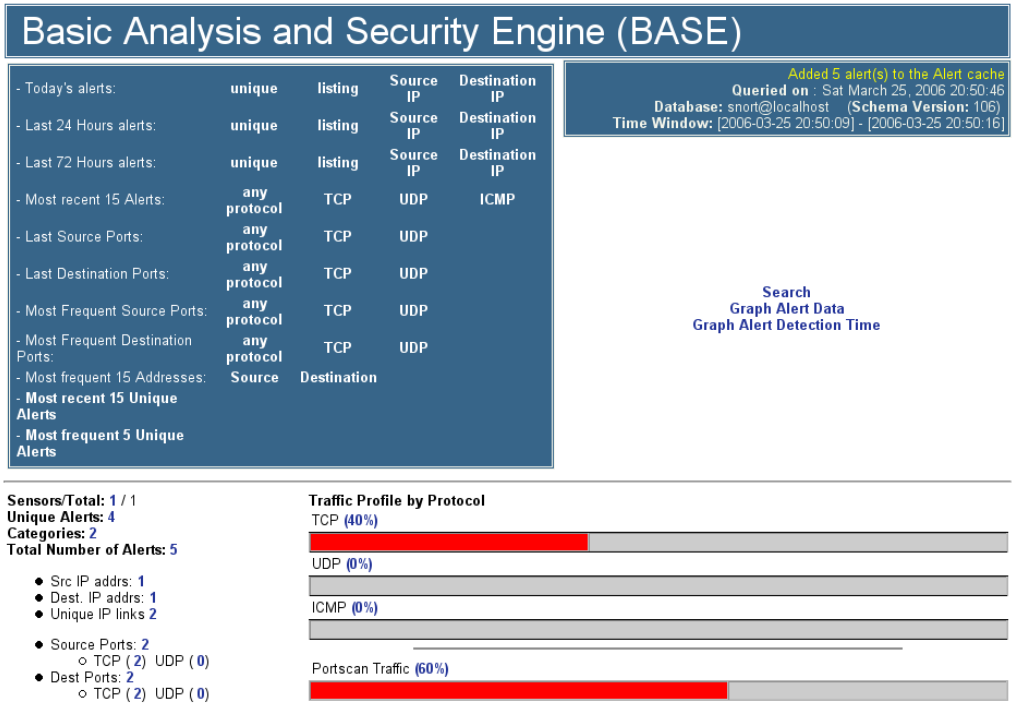


Figure 3-10 : Interface Web de Basic Analysis and Security Engine (BASE)

Pour terminer cette présentation de Snort et ces composants, nous dirons tout simplement que Snort est un très puissant outil connu comme un des meilleurs sur le marché, même quand il est comparé à des IDS et IPS commerciaux. Il a une plus grande communauté d'utilisateurs et de chercheurs (de nombreux plugins, frontends, consoles de management etc).
Sa mise en œuvre basique peut-être rapidement effectuée grâce notamment aux nombreux livres et documentations existants à son sujet.

Conclusion

Aujourd'hui, personne ne semble maitriser l'évolution des technologies de l'électronique et de l'informatique distribuée. Le tableau que nous peint les différentes études et statistiques de ce document nous édifient assez sur le caractère préoccupant que prend la sécurité informatique dans le monde et plus particulièrement en Afrique. Dans ce sombre décor, l'unique porte de sortie pour les entreprises et organisations demeure la conduite d'une véritable démarche sécuritaire aboutissant sans équivoque à la définition d'une stratégie de sécurité claire et adaptée ; elle-même, conduisant à la mise en application d'une politique de sécurité fiable et rigoureuse.

Dans ce contexte, les entreprises et organisations africaines en général et Ouest-africaines en particulier (la sous-région Ouest-africaine où nous avons pu réellement évaluer la situation de la sécurité informatique au sein des organisations) ont encore plus intérêt à prendre plus au sérieux leur « destinée informatique » car, comme nous l'avons démontré dans le document, même si nos systèmes et réseaux informatiques ne constituent pas des cibles de choix pour les cyber-délinquants, ils restent tout de même de bons candidats pour servir de bases intermédiaires aux attaques perpétrées contre les systèmes plus attrayants financièrement.

C'est pourquoi, nous recommandons à nos organisations africaines, de mettre en place non seulement des stratégies et politiques de sécurité, mais aussi d'adopter et d'y intégrer les nouvelles méthodes et systèmes de sécurité comme les sauvegardes hors sites, les plans de reprise d'activité et les systèmes de détection et de prévention d'intrusions.

Toutefois, même si une certaine maturité dans le domaine de la détection d'intrusion commence à se sentir, le plus important reste de savoir de quoi il faut se protéger. Les failles les plus répandues proviennent généralement de l'intérieur de l'entreprise, et non de l'extérieur. Des mots de passe simples, des droits d'accès trop élevés, des services mal configurés, ou encore des failles dans les logiciels demeure les bêtes noires en matière de sécurité informatique.

Ce document est l'aboutissement d'un travail de trois années. Sa réalisation nous a permis de découvrir et comprendre la véritable définition du travail en équipe c'est-à-dire la collaboration et la coordination. Nous avons certes rencontré des difficultés mais elles ne nous ont pas freinés. Au contraire, elles nous ont donné encore plus envie d'apprendre, de chercher et d'apporter notre pierre à l'édifice de la sécurité informatique.

Notre plus grand souhait, est de continuer nos recherches dans le domaine des systèmes de prévention d'intrusion et les algorithmes qui sont utilisés pour détecter les abus sur les systèmes d'information.

Après tout, on est tenté de se demander « A quand la sécurité à 100% ?

Glossaire

ACL : Access Control List.

Appliance : Se dit de toutes sortes de machines dont la principale caractéristique est de pouvoir être (théoriquement) simplement branchées pour fonctionner immédiatement de manière parfaitement opérationnelle. C'est souvent un dispositif (pare-feu ou IDS par exemple) contenu dans une boîte (souvent noire).

Audit : C'est une procédure de contrôle de la gestion d'une activité et de l'exécution de ses objectifs. En matière de systèmes d'information, l'audit de sécurité a pour objectif de mesurer l'écart entre la situation existante (sur les plans organisationnels, procéduraux et techniques) et la politique de sécurité de l'entreprise, les bonnes pratiques et l'état de l'art.

Auditeur : C'est celui qui contrôle le respect des procédures.

Auditabilité : Elle se définit comme la capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure à un événement (ordinaire ou exceptionnel) afin de déterminer s'il y a eu effectivement violation de la sécurité, et dans ce cas, quelles informations ou autres ressources ont été compromises. C'est aussi cette fonction qui est destinée à déceler et à examiner les événements susceptibles de constituer une menace pour la sécurité. Il s'agit là de l'objectif premier et majeur des systèmes de détection d'intrusion (IDS).

Authentification : Processus permettant de s'assurer de l'identité d'un utilisateur lors des demandes d'accès au Système d'Information.
Autorisation : L'autorisation d'accès est donnée au cas par cas à un utilisateur par une application en fonction des droits associés au rôle applicatif (ou par une ressource en fonction des privilèges).
Backbone : Colonne Vertébrale d'un réseau sur laquelle se raccordent divers éléments dont les sous-réseaux. On utilise aussi l'appellation d'épine dorsale. Ce tronc relie les équipements de concentration ou de commutation. En général il s'agit d'un réseau à haut débit (1 ou 10 Gigabits) qui relie entre eux les nœuds de commutation qui répartissent les données à travers une arborescence de petits réseaux.
Backup : (Sauvegarde) Enregistrement de fichiers sur un support autre que le disque dur (disquette, CD...). Le backup permet de récupérer vos données sauvegardées en cas d'erreur sur votre disque dur.
Bluetooth : Technologie de réseau sans-fil plutôt adaptée à l'interconnexion de périphériques. Bluetooth utilise la bande fréquence de 2,4 à 2,48 GHz et la technique FSK. La portée standard d'un équipement Bluetooth est de 10 m mais elle peut aller jusqu'à 100 m pour un débit asymétrique de 57,6 kbps / 723,2 Kbps ou symétrique de 433,9 Kbps. Un réseau composé d'un maître et de 7 esclaves peut être réalisé entre équipements Bluetooth, il est appelé Piconet. Il est possible d'interconnecter jusqu'à 10 Piconet pour former un Scatternet avec des interférences minimales.

Cheval de troie : Programme ou données qui semblent inoffensives lorsqu'elles sont chargées dans un système ou un réseau mais qui facilitent ensuite une attaque par un pirate ou un virus.
Chiffrement : Technique de codage des informations, généralement par transformation à l'aide de fonctions mathématiques, destinée à les rendre incompréhensibles par un tiers ne possédant pas les clés de la transformation
CLUSIF : Club de la sécurité de l'information français
Confidentialité : Prévention d'une divulgation non autorisée de l'information. Propriété qui assure que seuls les utilisateurs habilités ont accès aux informations.

CSI : Computer Security Institute
DDoS : Distributed Denial of service ou déni de service distribué.
DoS : Denial of Service. Déni de service. C'est une attaque destinée à paralyser ou ralentir un service (FTP, STMP etc) empêchant les utilisateurs autorisés à l'exploiter normalement. Il peut conduire à l'arrêt complet du serveur.
Firewall : Pare-feu. Equipement placé entre deux réseaux, généralement entre un réseau public et un réseau privé ayant pour mission de protéger ce dernier et de contrôler les paquets entrants comme sortants. Le contrôle est effectué par filtrage selon différents critères (IP, application, heure, contenu etc) ou authentification.
Flooding : Technique de piratage consistant à innonder un serveur en requêtes jusqu'à défaillance de celui-ci. Français: Raz de mare.
GFSI : Global Financial Services Industry
Hameçonnage : C'est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. 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, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Le hameçonnage peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.
HIDS : Host Intrusion Detection System
IDP : Intrusion Detection and Prevention
IDS : Intrusion Detection System
IPS : Intrusion Prevention System
IEEE : Institute of Electrical and Electronics Engineers
Intégrité : Elle permet que les informations et les logiciels sont complètes, exactes et authentiques. C'est l'intégrité qui peut nous assurer sur que le fait que les données sont effectivement ce qu'on croit qu'elles sont. Quand on parle d'intégrité réseau on fait référence aux procédures et techniques visant à garantir que les informations et données reçues sont bien celles qui ont été envoyées. Leur contenu doit être intégral et non modifié, les liens reliant des nœuds sources et des nœuds de destination devront aussi être valides.
Iptables : C'est la commande Linux qui permet à un administrateur de configurer Netfilter en mode Utilisateur.
ISO 27002 : Norme internationale constituant un « guide de bonnes pratiques » en matière de sécurité de l'information (anciennement ISO 17799:2005).
KERBEROS : C'est un protocole d'authentification réseau créé au Massachusetts Institute of Technology (MIT). Kerberos utilise un système de tickets au lieu de mots de passe en texte clair. Ce principe renforce la sécurité du système et empêche que des personnes non autorisées interceptent les mots de passe des utilisateurs.
Log : le terme log est notamment employé en informatique pour désigner un historique d'événements et par extension le fichier contenant cet historique ;
Mail bombing : Une attaque consistant à envoyer une avalanche d'e-mail sur le compte d'un utilisateur ou sur un serveur pour l'engorger.
Mainframe : Environnement informatique composé d'un système central et de stations clientes (exemple : IBM VM ou MVS).
MEHARI : Méthode harmonisée d'analyse des risques, développée par le CLUSIF. Voir http://www.clusif.asso.fr/mehari/.
Netfilter : C'est le module qui fournit sous Linux depuis la version 2.4 les fonctions de pare-feu, de partage de connexions internet (NAT) et d'historisation du trafic réseau. Iptables est la commande Linux qui permet à un administrateur de configurer Netfilter en mode Utilisateur.
NIDS : Network Intrusion Detection System

NIS : Network Information System. Nommé aussi *Yellow Pages* est un protocole client serveur développé par Sun permettant la centralisation d'informations sur un réseau UNIX.
Non répudiation : C'est le fait de ne pas pouvoir nier ou rejeter qu'un événement (action, transaction, tentatives d'accès à des ressources en réseaux…) a eu lieu. On associe souvent à ce critère de sécurité les notions telles que la journalisation, l'imputabilité, la traçabilité et éventuellement l'auditabilité.
Open-Source : C'est un concept qui incite les développeurs de logiciels à ne pas rendre leurs produits propriétaires et à inciter la communauté à ne pas hésiter à rentrer dans leurs codes afin de l'améliorer ou de l'adapter à leurs besoins. Souvent les logiciels *« Open-Source »* ou libres sont soumis aux termes de la licence d'utilisation GPL (General Public License) décrivant les conditions légales de l'utilisation, de la distribution ou la modification du code source.
Phishing : voir hameçonnage
Promiscuous : En français promiscuité. Il s'agit souvent en réseau informatique du mode promiscuité qui consiste pour un nœud du réseau de réceptionner tous les paquets qui passent par lui.
RADIUS : Remote Access Dial-In User Service. Protocole de gestion (client/serveur) d'accès à une base d'utilisateurs sur un serveur. Ce type de base de données utilisateurs est en particulier utilisé par les FAI pour authentifier les connexions sur leurs serveurs d'accès (BAS ou NAS), pour chaque utilisateur elle peut contenir les informations d'identifiant de connexion/mot de passe ainsi que adresse IP, plage horaire d'utilisation, etc.
RSSI : Responsable de la Sécurité des Systèmes d'Information « responsable du maintien du niveau de sécurité du Système d'Information. »
Sniffer : C'est un « analyseur réseau ». Il est appelé également analyseur de trames ou « renifleur ». C'est un dispositif permettant d'« écouter » le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent.
Sniffing : C'est l'acte d'analyser le réseau en écoutant et inspectant tous les paquets.
Snort : C'est un système de détection d'intrusion libre publié sous licence GNU GPL. A l'origine écrit par Martin Roesch, il appartient actuellement à Sourcefire. Des versions commerciales intégrant du matériel et des services de supports sont vendus par Sourcefire.
SYN : Synchronous idle. Etat de départ de l'établissement d'une connexion TCP.
SYN Flood : Saturation de paquets SYN. Attaque de type DoS qui a pour but de saturer la table de connexion TCP avec « n » connexions en attente d'ouverture et de « n » acquittements finaux du client.
Système d'information : SI. Représente l'ensemble des éléments participant à la gestion, au stockage, au traitement, au transport et à la diffusion de l'information au sein d'une organisation.
Virus : Programme intrus qui infecte les fichiers en y insérant des copies de son code, de sorte que ces fichiers deviennent « infectés ». Lorsqu'un fichier ainsi infecté est chargé en mémoire, le virus peut se propager à d'autres fichiers, et ainsi de suite. Les virus ont souvent des effets secondaires graves (parfois délibérés, parfois non). Par exemple, certains virus peuvent effacer le contenu d'un disque dur ou accaparer de la mémoire qui serait autrement utilisée par d'autres programmes.
Zombie : En sécurité informatique, c'est un ordinateur contrôlé à l'insu de son utilisateur par un pirate informatique. Ce dernier l'utilise alors le plus souvent à des fins malveillantes, par exemple afin d'attaquer d'autres machines en dissimulant sa véritable identité. Un zombie est souvent infesté à l'origine par un ver ou cheval de Troie.

Bibliographie

[RAM 07]	Cours : Détection d'intrusions réseaux avancées ; Durée: 30 heures ; Auteur: Ramblewski David ; Professeur à l'ESGI de Paris ; 03/12/2007
[AIN 08]	Cours sécurité avancée des réseaux ESGIS 2008 Alain Patrick AINA
[LIN 03]	Linux Server Hacks 100 Industrual-Strengh Tipsand tools ; Rob Flickener ; 2003 ; O'Reilly and Associates ; ISBN :0-596-00461-3 ; 225 pages.
[MAS 04]	Managing Security with Snort and IDSTools ; Kery JCox and Christopher Greg ; O'Reilly August 2004 ; ISBN : 0-596-00661-6 ; 288 pages.
[SNO 05]	Snort Cookbook ; Jabob Babbin, Simmon Biles, Angela D Orebagh ; O'Reilly, March 2005 ; ISBN : 0-596-00791-4 ; 288 pages.
[DEB 99]	Learning Debian GNU/LINUX by Bill McCarty ; 1st Edition September 1999 ; ISBN : 1-56592-705-2 ; 360 pages.
[STR 07]	Stratégies de sécurité ISO 27 0001 ; Conference DPM Sécurité des SI ; Marriot Champs Elysées Paris, 13 Juin 2007 ; Hervé Shawer.
[SEC 02]	Sécurité Internet : Mission sécurité ; B Dunsmore, J Brown, M. Cross, S. Cunnigham ; Edition: First Interactive, 13 Mars 2002 ; ISBN-10: 2844273033 ; 544 pages.
[BUI 02]	Building Secure Server with LINUX By Michael D. Bauer ; O'Reilly, October 2002 ; ISBN : 0-596-00217-3 ; 448 Pages.
[DAG]	Rapport de recherche ; Détection et prévention d'intrusion, présentation et limites ; Nathalie Dagorn ; Université de Nancy ; Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA) ; nathalie.dagorn@loria.fr; http://www.loria.fr/
[GREG]	Hack the Stack- Using Snort and Ethereal to Master the 8 Layers of an Insecure Network ; by Michael Gregg ; Syngress Publishing ; ISBN : 1-597-49109-8 ; 438 pages
[SNMA]	How to setup and secure Snort, MySQL and Acid on FreeBSD 4.7 Release ; english version ; 23 pages
[RAF 03]	Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID ; By Rafeeq Ur Rehman ; Publisher: Prentice Hall PTR ; Pub Date: May 08, 2003 ; ISBN: 0-13-140733-3 ; Pages: 288
[GIL 05]	Nessus Snort and Ethereal [S][2005] ; by Neil Archibald ; Gilbert Ramirez ; Noam Rathaus ; Josh Burke; Ed SYNGRESS ; ISBN: 1-59749-020-2 ; 472 pages
[ROM 05]	Projet :Mise en place d'une sonde ; Proposé par :Dr Mohamed ROMDHANI ; Réalisé par :M. Fathi BEN NASR, Mme Alia KHESSAIRI ABBASSI ; Année universitaire : 2004-2005
[STE 04]	Snort, MySQL, ACID, Apache, and Red Hat Enterprise Linux WS by Michael E. Steele ; Written By Patrick Harper, CISSP ; http://www.internetsecurityguru.com/; Document Version 6.1 ; Revised Date: April 7, 2004 ; 18 pages
[HAR 06]	Snort, Apache, SSL, PHP, MySQL, and BASE Install on CentOS 4, RHEL 4 or Fedora Core – with NTOP ; By Patrick Harper | CISSP RHCT MCSE with contributions and editing by Nick Oliver | CNE ; http://www.InternetSecurityGuru.com; Version 15 Page 1 of 19 Updated 8/17/2006 8:30 AM ; 19 pages
[GOM 08]	Snort Installation on SUSE 10.0 ; By Boris A. Gomez ; Universidad Tecnologica de Panama ; February 25, 2008 ; 17 pages
[MEN]	Snort® Installation, Configuration and ; Basic Usage ; Ed Mendez ; Director, Instructional Design & Development

Webographie

[INF]	Informatique http://fr.wikipedia.org/wiki/Informatique
[HIS]	Histoire des ordinateurs ; http://www.commentcamarche.net/contents/histoire/ordinateur.php3
[MON]	Montecito http://newsletteronline.net-free.fr/news/Les%20news%20du%2015_03_2005%20-%20%E9dition%20265.html
[CAT]	Catégories des réseaux sans-fils http://www.commentcamarche.net/contents/wireless/wlintro.php3
[STAT]	Statistiques du CERT http://www.cert.org/stats/cert_stats.html
[ATT]	Introduction aux attaques http://www.commentcamarche.net/contents/attaques/attaques.php3
[DAM]	Le cheval de Troie « Small.DAM » http://www.journaldunet.com/solutions/0701/070123-storm-ver-tempete-kyrill.shtml
[ATT 08]	Les attaques, JDN Mai,Juin 2008 http://www.journaldunet.com/solutions/securite/classement/l-etat-de-la-menace-informatique-dans-le-monde-juin-2008/la-pologne-pays-a-risque.shtml
[SEC]	Sécurité - Identification des risques et typologies de pirates http://www.commentcamarche.net/contents/secu/secuconn.php3
[ZOM]	Machine zombie - Wikipédia http://fr.wikipedia.org/wiki/Machine_zombie
[INT]	Intrusion informatique http://fr.wikipedia.org/wiki/Intrusion
[CAS]	Un cas d'intrusion informatique dans une usine de missiles coréenne http://www.journaldunet.com/solutions/breve/international/081002/
[MET]	Sécurité - Méthodologie d'une intrusion sur un réseau http://www.commentcamarche.net/contents/secu/secumet.php3
[PRE]	Premiers virus http://www.gerard-verhoest.com/securite.htm
[VIR]	Virus - Introduction aux virus http://www.commentcamarche.net/contents/virus/virus.php3
[PAR]	Pare-feu http://fr.wikipedia.org/wiki/Pare-feu
[CSI 07]	2007 CSI COMPUTER CRIME AND SECURITY SURVEY http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf
[GLO 07]	2007 Global Security Survey - The Shifting Security Paradigm http://www.deloitte.com/dtt/cda/doc/content/rs_Deloitte_Global_Security_Survey_2007.pdf
[MEN 08]	Menaces informatiques et pratiques de sécurité en France ; CLUSIF 19 Juin 2008 ; M. Laurent BELLEFIN ; Directeur de l'activité Sécurité ; Solucom Group http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2008.pdf
[GES 08]	LA GESTION DES RISQUES ; Concepts et méthodes ; CLUSIF https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-Gestion-des-risques-2008.pdf
[GES 07]	Gestion des identités 2007 https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-Gestion-des-identites.pdf
[MA 04]	Management de la sécurité de l'information - Une approche normative : BS7799-2 ; 2004 ; Business Continuity plan ; I.S. Strategy and recovery plan (disaster Recovery Plan) ; English version: November 2004 https://www.clusif.asso.fr/fr/production/ouvrages/pdf/Business%20Continuity%20Plan.pdf
[TES 04]	Test d'intrusion 2004 https://www.clusif.asso.fr/fr/production/ouvrages/pdf/TestIntrusion.pdf
[PLA 03]	Plan de Continuité d'Activité - Stratégie et solutions de secours du S.I. 2003 https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PlanContinuiteActivite.pdf
[PAN 08]	Panorama de la Cyber-criminalité - Année 2007 ; 2008 https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k7-fr.pdf
[RM 06]	RM & RSSI : Deux métiers s'unissent pour la gestion des risques du SI 2006 https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-RM-RSSI-GESTION-DES-RISQUES.pdf
[RSI 04]	RoSI - Retour sur investissement en sécurité des systèmes d'information : quelques clés pour argumenter 2004 https://www.clusif.asso.fr/fr/production/ouvrages/pdf/RoSI.pdf
[COM 05]	COMMISSION DES COMMUNAUTÉS EUROPÉENNES, Bruxelles, le 17.11.2005

	Livre vert sur un programme européen de protection des infrastructures critiques http://eur-lex.europa.eu/LexUriServ/site/fr/com/2005/com2005_0576fr01.pdf
[STR 07]	Stratégies de sécurité ISO27001 Conférence DPM sécurité des SI Marriott Champs-Elysées Paris, 13 juin 2007 http://www.hsc.fr/ressources/presentations/dpm-iso27/dpm-iso27.pdf
[PLA 03]	Plan de Continuité d'activité ; Stratégie et solutions de secours du S.I. ;Septembre 2003 ; Club de la sécurité des systèmes d'information français https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2007.zip
[ELA 04]	Élaboration de politiques de sécurité des systèmes d'information ; PSSI ; Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations ; Version du 3 mars 2004 http://www.ssi.gouv.fr/fr/confiance/documents/methodes/pssi-memento-2004-03-03.pdf
[AUD]	L'audit Informatique et la Qualité ; Bennani Samir ; Ecole Mohammadia d'Ingénieurs http://unpan1.un.org/intradoc/groups/public/documents/cafrad/unpan016352.pdf
[PRO 03]	PROJET PROFESSIONNEL ; Kevin FREOA ; Année universitaire 2002 - 2003 DESS Droit et Pratique du Commerce électronique ; Université Paris V René Descartes ; « La sécurité informatique dans l'entreprise » http://www.legalbiznext.com/droit/IMG/pdf/Freoa.pdf
[PCA]	Le plan de continuité d'activités PCA ; Franck Delbès, Senior consultant, Philippe Prunier, manager http://fr.country.csc.com/fr/ne/na/uploads/235_1.pdf
[PLAS]	PLAN DE SECOURS ET PLAN DE CONTINUITE DES OPERATIONS EN CAS DE CATASTROPHE OU DE DYSFONCTIONNEMENT André Adank http://www.aaconsultant.ch/image/Plaquetteservice.pdf
[PCA 04]	Le Plan de Continuité d'Activité (PCA / BCP) ; Comment le mettre en œuvre et vérifier qu'il restera opérationnel ? Bruno KEROUANTON ; RSSI Clear Channel France – CISSP ; 16 juin 2004 - Paris bruno.kerouanton.net/papers/netfocus2004-juin04-bk-**plan_continuite**.pdf
[PRO 08]	Problématique générale et enjeux d'un Plan de Continuité d'Activités http://www.sylog.com/fr/ressources/Marketing/Events/event_200801/slides/JBA_Prangins_17_janvier_2008.pdf
[DIS 05]	Disponibilité de l'information Plan de relève informatique ; Plan de relève corporative ; Copyright Jacques Bergeron 2005, adapté par Pascale Chaussé http://zonecours.hec.ca/documents/A20051570292.PlanscontinuiterelevePCVetudiants.ppt
[COM]	Comment gérer le risque lié aux intrusions? Etude des conditions de mise en place efficace d'un système de détection (IDS) Thierry Evangelista, Consultant Sécurité TURPIAL http://www.turpial.net/Docs/TURP_ChoixIDS.ppt
[STRPL]	Stratégie de sécurité: pensez long terme! http://www.zdnet.fr/actualites/informatique/0,39040745,39115928,00.htm
[DETP]	Pourquoi opter pour un système de détection des intrusions. http://www.zdnet.fr/actualites/informatique/0,39040745,2134409,00.htm
[6IDS]	6 IDS / IPS passés au peigne fin http://www.zdnet.fr/i/edit/tu/2004/12/tableau39193530.html
[DETI]	Les systèmes de détection d'instrusion : indispensables http://www.journaldunet.com/solutions/0207/020712_sonde_intrusion_1.shtml
[COMI]	Comment les systèmes de détection d'intrusion montent la garde http://www.zdnet.fr/actualites/informatique/0,39040745,39193530,00.htm
[CRTV]	CERT Statistics: Vulnerability Remediation http://www.cert.org/stats/vulnerability_remediation.html