Lab.RII **UNIVERSITÉ DU LITTORAL CÔTE D'OPALE**
Laboratoire Redéploiement Industriel et Innovation

DOCUMENTS DE TRAVAIL

N°93 **Janvier 2005**

Pierre E. EDORH

UNE SECURISATION GLOBALISEE DES SYSTEMES D'INFORMATION DE GESTION

GLOBALIZED SECURIZATION OF MANAGEMENT INFORMATION SYSTEMS

Pierre E. EDORH

Résumé : Depuis la fin de la décennie 1980, nombre d'organisations construisent ou se font construire leur site Web. Ce site peut, selon le cas, servir de support au commerce électronique en ligne, à la présentation de l'entreprise, à l'information sur celle-ci. Le site Web peut aussi servir de moyen de communication entre une organisation et ses filiales ou ses partenaires. Mais la connexion à l'Internet présente des risques, au sens où cette technologie constitue pour l'organisation l'ayant adoptée, une ouverture sur l'extérieur. Ceci se traduit par des dangers : piratages par jeux, espionnage concurrentiel, malveillance. Dans tous les cas, les menaces sont importantes et les coûts sont plus ou moins élevés : pertes d'exploitation, applications spécifiques et à la recréation des données. Cet article n'est pas doté d'exhaustivité. Il étudie les risques et les menaces d'attaques pesant sur les systèmes d'information de gestion des organisations et examine les mesures que ces organisations devraient prendre pour se doter d'un niveau élevé de protection (surtout dans le cadre d'un service Web).

Abstract: Since the end of the 80's, many organizations have built their own Web sites. These sites can be a support for the on-line commercial business or give information about the firm. Web sites can also be a communication tool between the entreprise and its subsidiaries or its partners. But Internet network is also a risk for the organization, since Internet Technology represents an opening of the organization to the environment, wich means new threats : games high jacking, competitive espionage, malevolent actions. In all cases, the threats are important and the costs are more or less high: operating losses, specific applications and data losses. Without pretending to exhaustivity, this paper studies the risks and attack threats which the management information systems is confronted to, and examines the measures that should be taken by these organizations to have a high level of protection (especially in a web service context).

UNE SECURISATION GLOBALISEE DES SYSTEMES D'INFORMATION DE GESTION

TABLE DES MATIERES

INTRODUCTION

Depuis la fin de la décennie 1980, nombre d'organisations construisent ou se font construire leur site Web[1]. Ce site peut, selon le cas, servir de support au commerce électronique en ligne, à la présentation de l'entreprise, à l'information sur celle-ci. Le site Web peut aussi servir de moyen de communication entre une organisation et ses filiales ou ses partenaires. Mais la connexion à l'Internet présente des risques, au sens où cette technologie constitue pour l'organisation l'ayant adoptée, une ouverture sur l'extérieur. Ceci se traduit par des dangers : piratages par jeux, espionnage concurrentiel, malveillance. Dans tous les cas, les menaces sont importantes et les coûts sont plus ou moins élevés. Ceux-ci sont liés par exemple, à des pertes d'exploitation, d'applications spécifiques et à la recréation des données. Des prévisions évaluent en milliards de USD[2], les coûts de la parade contre les risques et les menaces pesant sur la sécurité des systèmes d'information. A ce titre, selon Datamonitor, les dépenses mondiales des organisations en matière de sécurité informatique doubleront dans les trois prochaines années, pour se situer à 5,5 milliards de USD[3]. Cet article n'est pas doté d'exhaustivité. Il étudie les risques et les menaces d'attaques pesant sur les systèmes d'information de gestion des organisations et examine les mesures que ces organisations devraient prendre pour se doter d'un niveau élevé de protection (surtout dans le cadre d'un service Web).

Depuis le début de la décennie 2000, les risques et menaces susceptibles d'endommager les systèmes informatiques des organisations sont en croissance. Par exemple, les codes malveillants ou virus qui sont fabriqués et envoyés dans les réseaux informatiques deviennent très nombreux. Il est ici, permis de relever que, mensuellement, des centaines de nouveaux virus apparaissent au point qu'en avril 2004, il a été détecté 1400 nouveaux types de codes malveillants qui sont en guerre contre les systèmes d'information des organisations, dans le monde[3]. Ce constat se trouve corroboré par un adage susceptible d'effrayer toute personne disposant de fichiers sur un ordinateur ou connecté à un réseau ou à l'Internet : « le seul ordinateur sûr est celui qui est éteint, enfermé et enfoui à une profondeur de 20 pieds à un lieu tenu secret ».[4]

Cette insécurité informatique provient spécialement de pirates informatiques. Et, le piratage informatique est devenu un problème de société et un phénomène dont les manifestations sont en inquiétante augmentation. Par exemple, durant l'année 2000, on pouvait constater en Amérique du nord, que le nombre d'attaques quotidiennes, était quatre fois supérieur à celui de l'année 1999[5]. Cette recrudescence d'attaques de pirates s'étend en Europe (et dans le monde entier). En Europe, les attaques de pirates déplacent le balancier de la sécurité informatique vers des préoccupations primordiales. Ce constat s'appuie sur le résultat de l'étude faite par des chercheurs pour le compte de la société AVAYA, domiciliée aux Etats-

[1] Le Web est la désignation simplifiée de World Wide Web signifiant «toile d'araignée mondiale». Son équivalent est WWW ou W3. La toile d'araignée à laquelle on assimile l'Internet (International Network) ou encore réseau international en français, est aussi appelée le Net. Voir Balle (F.) et Cohen-Tanugi (L.) – sous la direction de – « *Dictionnaire du Web*. » Editions Dalloz, Paris 2001, p.296-297.
[2] L'USD désigne le dollar américain.
[3] Pritchard (S.) *« Dealing with the threat from within »*, in Financial Times, march 17 2004, p 04. Supplément I T Review, consacré à la sécurité des systèmes d'information.
[3] Foucart (S.) *« Les créateurs de virus informatiques deviennent des mercenaires »*, le Monde du 28 avril 2004, p.24.
[4] Elsbery (R.B.) *« The Spying game : how safe are your secrets ? »*, Office Systems. September 1999.
[5] Higgins (K.J.) *« Human element is key to stopping hackers »*, Information Week. May 29 2000.

Unis. D'après cette étude, portant sur 123 firmes européennes, 64% de celles-ci place les pirates au premier plan de leurs préoccupations en matière de sécurité informatique[6].

Il convient de souligner que les pirates informatiques utilisent plusieurs méthodes pour infliger des dommages aux systèmes informatiques des firmes. A ce niveau, nous pouvons mentionner trois types d'attaques de base, utilisées par les pirates : l'intrusion, la destruction et le refus de fonctionner. Chacune de ces attaques est souvent menée à l'aide de virus informatique. Par ailleurs, sur le Web, un stratagème préféré, employé par les pirates consiste à réorienter les clients fidèles d'une firme vers un site Web fantôme ou vers un site susceptible de parodier ou de critiquer la société concernée. Dans ce même esprit, un pirate peut perpétrer sur le site Web d'une entreprise, des actes obscènes ou malveillants ou nuire à la réputation d'une firme en faisant « exploser » son site Web. On ne peut que comprendre le caractère destructeur de la déflagration d'un site, par refus de fonctionner pour l'exploitation des transactions de commerce électronique (e commerce) des sociétés concernées par cette activité. Car un client faisant face à un site Web fréquemment hors d'usage, s'orientera purement et simplement vers un autre plus fiable[7]. Il devient alors important de protéger les informations confidentielles stockées ou envoyées à travers le système d'information des entreprises concernées. Par exemple, une société de crédit doit fournir l'assurance que les données sur sa clientèle telles que les informations sur les cartes de crédit, sont protégées. De même, les données relatives aux ventes et les secrets commerciaux, qui peuvent être volées, doivent faire l'objet d'une protection. Il va sans dire que toute firme effectuant des transactions sur l'Internet se doit de garder confidentiellement, les données sécurisées. Une organisation peut même être condamnée pour des dommages et intérêts si une incurie en matière de protection de son propre système d'information provoque des dommages à un tiers. La société fautive pourrait être tenue responsable des dommages causés[8], dont la source remonte aux pirates.

Les pirates informatiques n'appartiennent pas à une catégorie déterminée d'individus. On peut, sur ce point effectuer la segmentation suivante, en tenant compte de l'ordre de fréquence des attaques[9] :

- les salariés mécontents ;
- les pirates indépendants ;
- les concurrents nationaux ;
- les concurrents étrangers ;
- les pirates-mercenaires.

Ce dernier cas connaît une recrudescence dans les milieux professionnels[10]. Au demeurant, il convient de souligner qu'une partie importante des dommages causés aux systèmes informatiques des organisations et aux bases de données provient du personnel interne aux structures concernées. A ce titre, nous pouvons mentionner une étude réalisée par Gartner, selon laquelle 70% des accès non autorisés, constatés sur les systèmes d'information était effectué par des « initiés ». Et même plus préoccupant est le fait que 95% des attaques ayant provoqué des pertes financières ont été menées par des employés (en interne). On comprend alors, que malheureusement, les organisations ne peuvent plus considérer l'honnêteté de leur

[6] Shillingford (J.) *« Push-to-talk services gain ground »*, Financial Time (march 2004) op. cit. L'auteur cite l'étude réalisée par les chercheurs de GTMI, pour AVAYA, fournisseur d'équipements de télécommunication.
[7] Frolick (M. N.) *« A new master's guide to firewalls and security »*, Information Systems Management, Winter 2003, p.29-33.
[8] Franson (P.), *« Thwarting hackers »*, Electronic Business. May 2000.
[9] Keong (V.) *« The Ethical hack »*, C. A. Magazine. January/February 2000.
[10] Foucart (S.) (2004) op. cit.

personnel comme gratuite[11]. Les salariés mécontents des organisations peuvent créer de multiples dommages aux systèmes d'information de leur employeur, en choisissant, souvent un moment propice : la pose déjeuner[12].

En plus des délits commis par le personnel employé en interne, les organisations font face à l'action des pirates informatiques. Rappelons que ces pirates utilisent plusieurs méthodes pour accéder aux systèmes informatiques des organisations. Une de ces méthodes consiste à trouver des failles de sécurité[13] sur le système d'information. Cela peut concerner le serveur Web de l'organisation, qu'ils peuvent contrôler à distance et le site Web, dont ils peuvent modifier le contenu. Cet accès fournit aussi, la possibilité d'utilisation du serveur Web pour pénétrer dans le réseau interne de l'organisation. Et si des mesures adéquates ne sont pas prises pour contrer cette intrusion, un pirate peut accéder au matériel, aux fichiers, aux logiciels ainsi qu'à tout ce qui peut être volé, altéré ou détruit, avant toute réaction éventuelle de l'organisation. Dans cet article, nous nous proposons d'explorer les défis de la sécurité auxquels peuvent se confronter des professionnels des réseaux informatiques de gestion. Cela concerne aussi les professionnels du Web, lors de la mise en place et du maintient d'une présence Internet de leur organisation.

A cet effet, trois développements vont structurer cet article. D'abord, nous parlerons de virus et d'attaques informatiques et nous examinerons les fondamentaux des pare- feux (ou firewalls en anglais) et leur configuration. Il découle des limites de ceux-ci, une ouverture sur les réseaux privés virtuels (RPV) ou Virtual Private Networks (VPN) en anglais. Ensuite, nous parlerons des serveurs Web et de leurs vulnérabilités. Enfin, nous allons formulerons des suggestions pratiques, pour amorcer ou pour améliorer une politique globale de sécurité concernant le Web et les réseaux informatiques.

1. DES ATTAQUES AUX OUTILS DE SECURISATION

Dans un premier temps, nous ferons état des virus et attaques destinés à endommager les systèmes d'information. Dans un second temps, nous parlerons des moyens actuels utilisés pour sécuriser ces systèmes exposés.

1.1. LES VIRUS ET LES ATTAQUES INFORMATIQUES

Le but d'une attaque de pirate informatique n'est pas uniquement d'utiliser les failles de sécurité pour se connecter à un réseau pour y récupérer des données, mais d'en perturber le fonctionnement tant au niveau réseau qu'au niveau physique[14]. Ces attaques qui sont effectuées par des pirates informatiques, ont pour vecteur essentiel, les virus, encore appelés « codes malicieux » ou « codes malveillants ». Il est permis de souligner l'existence de trois types d'attaques de base, effectuées par les pirates : l'intrusion, la destruction et le refus de fonctionner. Par exemple, les pirates utilisent les virus de type « Cheval de Troie » tel que Netbus pour effectuer une intrusion. La destruction passe par l'utilisation de virus tel que « Sircam » (ou CodRed). Quant au refus de fonctionner, il est provoqué par l'utilisation du code malicieux de type Melissa (ou Nimda).

[11] Pritchart (S.) *"Dealing with the threat from within"*, Financial Time (March 2004) op. cit.
[12] Janss (S.) *«Frontier defense: personnal firewalls software »*, Network World. August 7 2000.
[13] Foucart (S.) (2004) op. cit.
[14] Males (D.), Pujolle (G.) *« WI-FI par la pratique ».* Editions Eyrolles, Paris 2004, p.119.

Le nombre de codes malicieux en circulation sur les réseaux informatiques est en forte croissance, surtout, depuis le début de la décennie 2000. Si durant l'année 2003, l'Internet a connu une forte activité virale informatique, avec une moyenne mensuelle de 400 souches de codes malicieux nouvellement apparus, l'année 2004 a connu une statistique supérieure. Par exemple, en janvier 2004, à peu près 600 codes malins ont été détectés. Cette progression de codes malveillants s'est poursuivie durant le trimestre au point qu'en avril 2004, environ 1400 nouveaux codes ont été détectés sur l'Internet[15]. Et, les dernières familles de ces virus apparus sur ce réseau (Mydoom, Netsky et Bagle) sont davantage virulentes, résultant d'un professionnalisme accrû de la part de leurs créateurs. Ces derniers ne sont plus ces jeunes programmeurs ou étudiants, voulant démontrer un exploit, en écrivant un programme original pour se faire remarquer.

Ces créateurs de virus sont devenus de véritables professionnels, travaillant sur leurs créatures « comme sur de véritables projets informatiques », liés à des activités délictueuses comme l'envoi gigantesque de publipostages électroniques non sollicités ou Spams. Ces envois sont effectués frauduleusement et anonymement sur la base de la collette déloyale et illégale de courriels. Les nouvelles versions de codes malicieux sont davantage virulentes : utilisant des failles de sécurité, elles peuvent déclencher des infections d'appareils en dehors de toute action de leurs utilisateurs. Soulignons que ces virus peuvent cacher des logiciels qui, activés à distance, sont capables de collecter par exemple, des fichiers de courriers électroniques, des mots de passe et même des informations de caractère bancaire comme les numéros de cartes bancaires. C'est faisable par le biais d'un logiciel espion qui capte les frappes clés de l'utilisateur[16]. Cela s'appelle la méthode des « Keyloggers ». C'est de cette façon qu'en 2004, en région parisienne, des pirates sont parvenus à détourner les comptes des clients de la banque Société générale[17]. Une autre forme d'attaque appelée « vol de session », utilisée par les pirates, consiste à profiter d'une faille de sécurité pour pénétrer à distance, à l'intérieur d'un appareil (un serveur par exemple), pour y récupérer des informations sensibles tels le code et le mot de passe des utilisateurs. Nous pouvons ici souligner des imperfections liées aux codes informatiques. Par exemple en France, les experts de la sécurité informatique considèrent souvent que les codes des cartes bancaires, réduits à seulement quatre caractères, ne présentent pas du tout, un niveau de sécurité suffisamment élevé.

Devant ces risques et menaces susceptibles d'occasionner des dommages aux systèmes d'information des organisations, il est opportun et urgent de mettre en place des solutions de sécurité. Celles-ci, agissant contre les attaques d'origines internes et externes à une organisation, renvoient, selon nous, à plusieurs outils que nous allons étudier respectivement.

1.2. LES PRINCIPAUX MOYENS DE SECURISATION

Nous parlerons, d'une part, des firewalls (ou pare-feux en français) et d'autre part, des Virtual Private Networks (VPN) ou réseaux privés virtuels. Ces outils nous paraissent être adaptés, actuellement, à une sécurisation des systèmes d'information, contre les attaques, initiées par des esprits malveillants.

[15] Foucart (S.) (2004) op. cit. L'auteur cite les estimations établies par l'éditeur de logiciels antivirus TrendMicro.
[16] Taylor (P.) *« Keep out my inbox »*, Financial Time (March 2007) op. cit. p. 08
[17] Durant (J.) et Maussion (C.) *« Bracage de banque sur le Net »*, Libération du 20 août 2004, p. 12

1.2.1. LES FIREWALLS : OUTILS DE SECURISATION

Cette technologie tient à la mise en place de logiciels et / ou de boîtiers, disponibles sur le marché. Ces outils limitent la circulation des données à un réseau privé, afin d'y garantir la sécurité. Le firewall, constituant un système de gestion et de contrôle de trafic de données entre deux réseaux, doit être installé à tous les points de contact entre le réseau interne de l'organisation et l'extérieur. Le firewall a pour fonction essentielle d'inspecter les données pénétrant à l'intérieur du réseau de l'organisation et provenant par exemple de l'Internet[18] ou d'un système d'échange de données avec les clients ou les fournisseurs - par exemple l'Extranet.[19] Au demeurant, on peut indiquer ici, que la mise en place de firewall constitue la première mesure à prendre pour sécuriser un réseau informatique[20]. Les sociétés commerciales et les organismes de recherche connaissent souvent une utilisation importante d'ordinateurs. De ce fait, les environnements de ces structures disposent souvent de firewalls. En pratique, un grand nombre de petites sociétés, soit ne disposent pas de firewall, soit croient à tort qu'elles jouissent d'une protection offerte par leur fournisseur de service Internet ou en anglais Internet Service Provider (ISP). Ces petites sociétés comptent aussi à tort, sur leur routeur.

Nous pouvons mettre en exergue plusieurs catégories de firewalls[21]. Un firewall périphérique, qui constitue le type de pare-feu le plus simple, a un fonctionnement peu compliqué. Il examine les messages traversant le réseau et bloquera ceux qui ne présenteront pas le degré de sécurité requis. Dans sa plus simple configuration ce filtre de paquets examine d'abord, l'adresse IP (Internet Protocol) de l'émetteur et du destinataire sur le paquet, compare l'adresse avec celles figurant sur une liste agréée à l'intérieur du routeur du firewall. Ensuite, ce filtre, soit autorise l'accès, soit, refuse au paquet, la possibilité d'aller plus loin[22]. Néanmoins, on peut relativiser l'efficacité des firewalls en indiquant que 30% des sites Internet ayant subi des attaques était pourvu de firewall[23]. Car les pirates informatiques connaissent les vulnérabilités des protections de sécurité traditionnelle tels que les firewalls-filtres de paquets et peuvent utiliser ces vulnérabilités pour contourner les protections installées. Ce premier type de firewall est vulnérable à la reconnaissance IP par laquelle un pirate utilise une adresse IP légitime pour infiltrer la protection du firewall[24].

Une autre configuration de firewall, qui est davantage préférable au firewall périphérique, est connue sous l'appellation de « Zone démilitarisée » - ou Demilitarized Zone (DMZ) en anglais. On y connecte des appareils présentant un risque de piratage élevé[25]. Dans cette configuration, le serveur Web de l'organisation et d'autres serveurs, pouvant être, depuis l'extérieur, attaqués - serveur de messagerie, serveur de fichiers File Transfer Protocol (FTP) - , sont placés entre deux firewalls. Dans cette situation on place un firewall robuste entre le serveur Web et le réseau de l'entreprise ou de l'organisation. Ce firewall protège le réseau interne de la structure considérée contre les attaques lancées à partir du serveur Web. Ce

[18] Finez (L.) *« Sécurité informatique »,* Magazine FACE, Chambre de commerce et d'industrie de Lille, février 2003, p.29.
[19] On parle d'Extranet, lorsque le réseau Intranet d'une organisation est interconnecté au réseau Internet, pour offrir des services aux partenaires externes à l'organisation
[20] Royer (J.-M.), *« Sécuriser l'informatique de l'entreprise : enjeux, menaces, prévention et parades »*. Edition ENI, Nantes 2004, p.53.
[21] Voir *« Firewall Guard Perimeter »,* Security. June 1999.
[22] Frolick (M. N.), (2003), op.cit.
[23] Golman (J. E.) *« Applied Data Communications. A business Oriented Approach »,* Wiley 1998.
[24] Kuipers (F.) *« Preventing the Hack Attack »,* Telecommunication. July 2000.
[25] Royer (J.- M.), (2004), op. cit., p.55.

faisant, les bases de données et d'autres données sensibles de la structure sont mieux protégées avec un avantage supplémentaire : le firewall peut empêcher les employés mécontents d'attaquer le serveur Web, depuis l'intérieur de la structure considérée.

Mais qu'en-t-il des attaques émanant directement de l'Internet? Une réponse appropriée est fournie en installant un routeur, configuré comme un filtre de paquets, entre l'Internet et le serveur Web. Ce routeur est censé bloquer le trafic Internet qui n 'est pas autorisé ou dirigé vers le service du serveur Web Hypertext Transfer Protocol (HTTP). On comprend que ces deux firewalls créent, à la fois, cette DMZ, dans laquelle doit passer tout trafic, à destination ou en provenance de l'extérieur. Aucun trafic ne peut circuler à l'intérieur ou à l'extérieur de la DMZ, sans passer par un « système de contrôle d'accès ». Ce mécanisme de contrôle d'accès rendant la DMZ efficace, est filtrant au sens où la DMZ inspecte la demande entière pour des données, au lieu d'examiner uniquement les adresses de la source et de la destination. Les connexions entre les clients demandeurs et les serveurs sont créées après que la DMZ ne soit satisfaite de légitimité de la demande. L'utilisation de filtres sophistiqués de certaines commandes spécifiquement utilisés par les pirates informatiques pour sonder et attaquer les systèmes d'information est alors identifiée, piégée et détruite[26]. Ce qui veut dire que les requêtes HTTP, dirigées sur le serveur Web ainsi que d'autres applications TCP/IP (Transfer Control Protocol/Internet Protocol) telles que SMTP (Simple Mail Transfer Protocol), MIME (Miltipurpose Internet Mail Extension), Telnet, FTP, Gopher, Real et Audio peuvent être tous triés. Si un paquet contient une signature d'attaque connue ou un code suspect, la transaction sera alors refusée.

Il existe un troisième type de firewall faisant l'objet d'une utislisation croissante, mais controversée : le firewall partagé (ou distribué). Ces firewalls examinent les paquets et permettent ou refusent les accès, juste à la manière des firewalls périphériques. Mais, ils sont localisés sur chaque poste de travail ou chaque serveur. L'avantage de ce système réside dans le fait que, le firewall du poste de travail ou du serveur devient une ligne de protection si le firewall périphérique devient non opérationnel. Aussi, le firewall distribué devient-il réducteur de la menace des attaques effectuées par des initiés (personnel interne à l'organisation). Cela s'effectue simplement en isolant les plus petits groupes d'utilisateurs. A travers les outils de contrôle des firewalls, les accès à certains appareils peuvent être limités aux employés ayant un besoin d'accès. En limitant le nombre de personnes pouvant accéder au segment d'un réseau, on réduit la probabilité qu'un des salariés autorisés à l'accès soit l'employé mécontent voulant détruire les archives de l'organisation considérée ; la principale critique formulée à l'encontre du firewall partagé, destiné à protéger un serveur Web est que le Webmaster contrôle le serveur. Les experts de la sécurité informatique arguent que le firewall d'un serveur Web a une durée de vie courte. Et le webmaster est certain de détruire la configuration du firewall, lorsqu'il modifie globalement, l'ensemble du site[27].

Somme toute, l'installation, la configuration et la maintenance rationnelles de firewalls sont déterminantes dans la protection du matériel, des logiciels et des données. Cependant, il est permis d'indiquer que la mise en place d'un firewall, destiné à sécuriser les échanges de données entre réseaux, contre les attaques, ne garantit pas, dans tous les cas de figure, une sécurité totalement satisfaisante. Devient alors nécessaire, la mise en place d'une autre solution. Celle-ci tient à une autre technologie dénommée : les Virtual Private Networks (VPN) ou réseaux privés virtuels.

[26] Golman (J. E.), op. cit.
[27] Messmer (E.) *« Second line of defense »*, Network World. July 2000.

1.2.2. LES VPN : TECHNOLOGIE DE SECURISATION

Le firewall est normalement, destiné à protéger un système d'information contre d'éventuelles attaques. Cependant, si une organisation dispose d'au moins deux sites distants, reliés par l'Internet, les données échangées peuvent alors, être consultées, modifiées ou supprimées, si leur sécurisation fait défaut[28].

Le VPN est une technologie relativement récente sur le marché de la sécurité informatique. Par ce réseau on peut sécuriser l'échange de données entre au moins deux sites distants. Le VPN garantit les identités de l'expéditeur et du destinataire. Elle garantit aussi l'inviolabilité des données, leur intégrité ainsi que la certitude de leur acheminement et de leur réception. Le trafic concerné transite par le réseau privé (et non, par l'Internet public)[29]. De ce fait, la technologie VPN, proposée en option sur chaque site, par des fabricants en concurrence sur le marché de ces produits, permet de chiffrer et d'authentifier le trafic IP. Les VPN sécurisent complètement et conséquemment, les échanges d'informations de l'organisation, à partir du siège, jusqu'à la filiale (ou jusqu'aux filiales). Cette configuration est aussi faisable, tant, dans le cas des relations liant le siège d'une organisation et ses partenaires (dans le cadre des sites Extranet) que dans celui des relations entre le siège et les commerciaux mobiles ou même dans le raccordement de télé-travailleurs[30].

Mais, au vrai, comment fonctionne le système ? Pour cette technologie VPN, selon le modèle retenu, le chiffrement s'effectue au niveau de la couche réseau. Ceci se traduit par le fait qu'aucune information ne sera visible sur la partie publique (sauf les adresses IP du firewall-source et du firewall de destination). Une autre conséquence de ce chiffrement est que l'on peut crypter, au choix, soit des échanges entre deux réseaux, soit des échanges établies seulement entre certaines machines. A ce niveau, il va de soi que les règles de sécurité pour les autorisations/interdictions des accès, définies au préalable, sur le firewall, restent valides, indépendamment de la fonction VPN[31]. Les VPN constituent de fait, des moyens technologiques améliorant la sécurité des échanges de données ou d'informations entre au moins deus sites distants.

Au demeurant, la protection des VPN peut être élargie. Et elle concerne aussi, les réseaux sans fil ou les Wireless Fidelity (WI-FI) en anglais. Selon l'architecture du système informatique d'une organisation, les WI-FI peuvent faire partie des réseaux de cette dernière. Les WI-FI fonctionnent via les ondes. L'utilisation des WI-FI procure un avantage au sens où, n'importe quel utilisateur peut se connecter, en quelques secondes, au réseau. Cet utilisateur peut même se mouvoir au sein de la firme, de bureau en bureau, à l'aide d'un portable[32], sans compromettre la qualité des données, dans le réseau informatique. Cependant, l'utilisation des WI-FI, présente des inconvénients. Car les ondes (de radio) ne possèdent pas de barrière ou de limite physique : l'environnement immédiat externe d'une organisation peut recevoir ces ondes. Et les pirates informatiques qui souhaitent attaquer son réseau, peuvent le faire beaucoup plus rapidement à distance, en s'introduisant dans le WI-FI, par le biais d'un point d'accès ou Access Point (A P) en anglais. On comprend que cette situation des WI-FI demande une sécurisation. Celle-ci, au départ, se fondait sur le cryptage, par le biais du

[28] Selon les termes des documents techniques de la société NETASQ, spécialisée dans la sécurité informatique. Cette société est située à Villeneuve d'Ascq, en France.
[29] Finez (L.) op. cit.
[30] Plouin (G.) Soyer (J.), Triouller (M. E.) *« Sécurité des architectures Web »*. Editions Dunod, Paris 2004, p.280-281.
[31] Selon les documents techniques de NETASQ, op. cit.
[32] Royer (J.- M.), (2004) op. cit., p.104-105.

protocole Wire Equivalent Privacy (WEP), qui, en français, peut être désigné par l'expression suivante : « Niveau de sécurité équivalent à celui d'un réseau câblé ». Le WEP assure la sécurisation des communications circulant sur toutes les ondes. Cependant, il est permis de souligner que les pirates informatiques ont finalement violé le WEP, dont le niveau de sécurité est devenu inférieur à celui d'un réseau câblé traditionnel[33]. Il est apparu nécessaire de trouver des parades. Celles-ci tiennent alors à la mise en place de VPN, avec des pare-feux. Les VPN, apparus comme le moyen le plus fiable de sécuriser un réseau sans fil, demeurent à l'heure actuelle, la méthode la plus utilisée. Et l'utilisation de VPN permet, entre autres possibilités, d'identifier, d'autoriser l'accès tout comme le chiffrement de tout trafic circulant dans le réseau[34].

Globalement, au-delà des inconvénients liés aux VPN (qui exigent, par exemple, davantage de compétences,…), on peut élargir les avantages liés à cette technologie : la mise en œuvre est rapide, les coûts sont plus réduits et, rappelons–le, le chiffrement assure la sécurité. De plus, l'utilisation des VPN autorise une plus grande flexibilité, en cas d'évolution et de nouvelles implantations (redéploiements en réseaux,…). Enfin, l'installation des VPN permet une rapidité des accès nomades, grâce à l'utilisation des technologies émergeantes (ADSL,...).[35] Le serveur Web, son installation et son exploitation constituent une composante cruciale d'une stratégie de protection globale des réseaux informatiques. Il convient d'en faire état.

2. LA PROTECTION DU SERVEUR WEB

Dans une organisation connectée à l'Internet, il est nécessaire de protéger le serveur Web. Le bien-fondé de cette protection particulière accordée à un tel appareil réside dans le fait que, dans ce cas de configuration, le serveur Web se trouve ouvert à tout le trafic Internet. Cela est d'autant plus vrai quand on sait que 80% des codes malicieux actuels pénètrent dans le système d'information des organisations à partir de l'Internet, pour y ravager les réseaux, réduire la productivité et détruire les données informatiques vitales. De ce fait, le serveur Web constitue souvent, la voie royale par laquelle s'effectuent les attaques des pirates informatiques.

Par conséquent, le serveur Web devrait être totalement séparé des autres serveurs faisant fonctionner d'autres applications[36]. A des fins de sécurité maximale, le serveur Web devrait être configuré comme un « bastion », au sens où il est fortifié contre les attaques, du fait qu'il se trouve dépouillé de tous les services et logiciels non essentiels . Seuls les documents et scripts utilisables y seront installés. Conséquemment, le serveur Web est isolé du reste du réseau de l'organisation. L'utilisation de ce type de serveur demande une autre précaution, consistant à y restreindre, le plus possible sévèrement, l'accès à quelques utilisateurs. En fait, dans l'organisation, le directeur des systèmes et les gestionnaires du Web devraient y avoir accès. Seuls quelques utilisateurs devraient accéder au système : les personnes ayant la plus faible probabilité d'y commettre une erreur et d'y introduire un danger ou d'y utiliser un mot de passe erroné.

[33] Idem, p. 105.
[34] Males (D.) et Pujolle (G.) *« WI-FI par la pratique »* . Edition Eyrolles, Paris 2004, p. 134-135
[35] Corvalan (R.), Corvalan (E.) et Le Corvic (Y.), *« Les VPN : principes, conception et déploiements des réseaux privés virtuels »*. Editions Dunod, Paris 2003, p. 24.
[36] Gips (M. A.) *« Is your site a hacker's delight ? »*, Security Management. August 1999.

Derrière la protection du serveur Web, permise par sa séparation des autres applications, se profile une autre protection. Celle-ci tient à des considérations relatives à l'utilisation rationnelle de serveur Web, à la protection du site hébergé, à la protection des systèmes d'exploitation et à l'utilisation de logiciels défensifs.

2.1. L'UTILISATION RATIONNELLE DU SERVEUR WEB

L'utilisation rationnelle du serveur Web relève d'une démarche de sécurité concernant certaines données. Par exemple, dans une organisation, on se doit d'éviter d'introduire, dans le serveur Web, des données confidentielles telles que les données comptables. A des fins de sécurité, le serveur Web devrait être utilisé pour des services Web, et non pour d'autres services liés à l'Internet tels que Telnet, qui permettent aux utilisateurs d'exploiter leurs ordinateurs, depuis un endroit éloigné. L'augmentation de plus en plus importante du nombre d'utilisateurs mobiles et d'utilisateurs de télécommunications connectés à distance aux réseaux de leurs organisations accroît la vulnérabilité des systèmes d'information.[37] Par ailleurs, Telnet peut constituer un autre point d'entrée pour les pirates qui utilisent simplement un nom de code et un mot de passe. Et les logiciels aidant les pirates à obtenir les noms de code et les mots de passe[38] sont tous les jours, davantage sophistiqués. A cet égard, certains techniciens et experts en sécurité informatique savent que nombre de mots de passe utilisés sont si simples qu'un pirate peut facilement les deviner. On peut, à ce titre, citer quelques exemples. Sur le Web, un consultant de Chicago était capable de pénétrer plus d'une centaine d'ordinateurs de ses clients. Cela était rendu possible par le fait que ses clients avaient tous choisi comme mot de passe, « Bull 5 », une variante du nom de l'équipe des « Chicago Bulls », évoluant en première division en basket-ball, aux Etats-Unis à la National Basket-ball Association (NBA). De plus des techniciens en sécurité informatique ont trouvé que les administrateurs de réseaux utilisent souvent le mot « God » (qui, en français, signifie Dieu) dans leur mot de passe. D'autres mots apparaissent dans les mots de passe, communément utilisés. On pense notamment à « Secret » c'est-à-dire, secret et « Password », qui veut dire mot de passe[39]. Et les pirates ainsi que les espions le savent. C'est la raison pour laquelle, ils l'utilisent à leur avantage.

La protection du serveur Web ne saurait être réduite à son utilisation rationnelle. Cette protection peut être étendue au site Web hébergé.

2.2. LA SECURITE DU SITE HEBERGE

Il arrive fréquemment qu'une organisation fasse héberger en externe son site Web. Une organisation utilisant un fournisseur d'accès à l'Internet ou en anglais, Internet Service Provider (ISP) pour l'hébergement de son site doit faire preuve de la plus grande circonspection, dans le choix de son fournisseur. Le petit fournisseur de service « du coin de la rue » peut réaliser des prestations moins onéreuses pour l'hébergement de site; mais il ne pourra probablement disposer davantage de ressources pour assurer la sécurité appropriée de ses clients. Il est permis de préciser que l'hébergement d'un site Web par le biais d'un ISP permet des avantages. Séparer physiquement, la fonction Web des locaux de l'organisation, permet de s'assurer que des « systèmes critiques » seront insensibles à des interruptions de services, provoquées par une attaque de pirates, lancée à partir de l'Internet. En décidant de louer les services d'un ISP pour héberger son site Web, les dirigeants d'une organisation

[37] Franson (P.), op. cit.
[38] Logiciels appelés en anglais « crackers » et « snifers ».
[39] Elsberry (R.B.), op. cit.

doivent rechercher un fournisseur parmi les sociétés proposant l'hébergement d'application et de gestion de site Web. Ces sociétés d'hébergement prennent la responsabilité de tous les problèmes du site, y compris sa sécurité. Mais, ce type d'hébergement est onéreux. Il le serait probablement, d'ailleurs au titre que le montant de la facture établie par un consultant (extérieur), appelé en urgence pour effectuer des travaux, à la suite d'une infraction majeure, constatée sur les systèmes d'information d'une organisation. Quel que soit le type d'organisation sous-traitant l'hébergement de son site Web, il lui faut prendre une autre précaution : éviter des serveurs d'hébergement communautaire (afin d'avoir une maîtrise de son réseau). Et de ce fait, l'organisation concernée devrait préférer les serveurs dédiés dans les zones réseaux qui lui sont réservées[40].

Nous considérons, pour notre part, sur la base de notre expérience professionnelle, que même si un site Web d'une organisation est hébergé, il n'est pas rigoureusement et totalement, à l'abri de risques et d'attaques. Et les menaces ou attaques susceptibles de causer des dommages au système d'information de l'organisation peuvent alors, venir de l'intérieur. Cela peut émaner par exemple, soit de supports infectés par un virus (disquettes, CD-ROM,…), utilisés par un salarié interne imprudent, soit d'un salarié mécontent. Par conséquent, nous pensons que le fait de faire héberger le site Web de l'organisation, ne doit pas dispenser les responsables de l'organisation, de prendre des mesures de sécurité conséquentes. Celles-ci peuvent relever de l'utilisation adéquate d'antivirus. Il est vivement conseillé d'installer sur les réseaux informatiques, des antivirus puissants, existant sur le marché, pour protéger les réseaux informatiques. Ces antivirus constituent un dispositif spécialisé, interceptant les virus à la passerelle d'accès avant leur pénétration dans les réseaux d'une organisation. Selon la configuration, on peut par exemple, insérer l'antivirus entre le firewall et le réseau informatique. Selon le cas, l'antivirus toujours mis à jour, balaye tout le trafic entrant et sortant, à la recherche de virus et protège le réseau, à la passerelle d'accès, au lieu de compter sur la protection de l'ordinateur de bureau seul. Car certains utilisateurs peuvent déconnecter la protection de leur ordinateur de bureau[41]. En installant l'antivirus, si un virus parvient à pénétrer dans le réseau, ce dispositif réduit les problèmes de fiabilité et d'intégrité, empêchant les utilisateurs d'envoyer ledit virus aux partenaires ou aux clients de l'organisation.

L'antivirus puissant donne des avertissements d'activité virale, en envoyant un avis d'alerte par courriel[42] à l'administrateur, en cas d'interception d'un virus. Les administrateurs disposent d'un registre signalant, non seulement chaque incident relatif à des attaques virales d'origine extérieure, mais aussi tous les cas dans lesquels, des utilisateurs internes tentent d'envoyer des fichiers infectés. Les antivirus sont certes, des dispositifs indispensables, en matière de sécurisation des systèmes d'information. Mais, il n'en demeure pas moins vrai, qu'en matière de sécurité informatique les systèmes d'exploitation méritent une attention particulière.

2.3. LES SYSTEMES D'EXPLOITATION

Dans le cadre de la sécurisation d'un serveur Web, il devient adéquat de soulever un thème important : le choix du système d'exploitation, configuré pour gérer le logiciel d'applications et de serveur. Même si le serveur Web est bien protégé, des dangers peuvent provenir de la mise en place du système d'exploitation. De nombreux système d'exploitation peuvent fonctionner sur les serveurs Web. Parmi les plus dominants, on peut citer Windows NT et

[40] Camborde (C.), *« Sécuriser vos applications Internet »*. Edition Dunod, Paris, p.92.
[41] Ou même oublier de mettre à jour, leurs fichiers modèles ou leur moteur de recherche.
[42] Ou Email (courrier électronique)

UNIX. L'efficacité de chacun des deux, peut être discutable selon les experts et selon les utilisateurs. Seule, une configuration correcte de chaque système d'exploitation et de son installation peuvent le faire fonctionner à un niveau de sécurité le plus élevé[43]. De plus, s'impose un renforcement du système d'exploitation. Par exemple, après l'installation de firewall[44], on doit vérifier que le système d'exploitation est mis à jour contre les bogues et les failles de sécurité. Sinon un pirate actif peut les exploiter, quelque soit le type de firewall. Par ailleurs, quel que soit le système d'exploitation choisi, lors du démarrage d'une application Web, il est conseillé de prendre un certain nombre de précautions de bons sens :

- ne pas créer d'utilisateur inutile ou d'utilisateur avec un mot de passe simple ;
- ne pas activer des partages réseaux inutiles ;
- ne pas installer des services inutiles (tels que FTP, Telnet,…) ;
- ne pas laisser des mots de passe par défaut, pour serveurs applicatifs.

Pour le cas du système d'exploitation Windows NT, il est permis d'observer des précautions suivantes :

- protéger le compte administrateur. On doit, à ce titre, éviter les connexions « administrateur » depuis l'extérieur ;
- protéger le Security Access Manager (SAM), base de données comportant les mots de passe. C'est dangereux pour une organisation de se voir voler ce fichier par un pirate. Car ce dernier prendra possession de la liste des comptes et des mots de passe[45]

Un sens élevé de responsabilité et de veille peut conduire les responsables informatiques d'une organisation à anticiper la survenance d'une attaque menée par un pirate informatique. On peut alors, élargir la sécurisation des systèmes d'information en recourant à des simulations, permises par des logiciels défensifs.

2.4. LES OUTILS LOGICIELS DEFENSIFS

Pour des considérations de sécurisation optimale, en plus de la mise jour de son système d'exploitation pour faire face aux menaces, une organisation peut mettre en place, nombre d'outils logiciels. Les outils de détection d'intrusion peuvent surveiller l'activité du réseau, en contrôlant les paquets, pour des exemples d'activité anormale, identifier les signatures d'attaques électroniques connues et les abus, pour alerter le personnel concerné en cas de détection d'une telle activité. La technologie de détection d'intrusion permet à l'organisation de déterminer l'auteur de l'intrusion et la fréquence[46] de ses délits. Nous pouvons, à ce niveau, donner l'exemple du scanner de vulnérabilités qui, actuellement, constitue un bon outil de détection de défaillances. Cet outil contrôle le serveur Web, à la recherche de vulnérabilités, occasionnées à la suite d'une mauvaise configuration.

S'il est bien utilisé, ce scanner indiquera comment le serveur devra être reconfiguré, pour combler les lacunes de vulnérabilité. Ces scanners peuvent devenir des outils offensifs en imitant l'attaque d'un pirate, par une tentative simulée de pénétrer le serveur Web. Ce faisant, ces scanners peuvent y identifier les faiblesses. Il n'est pas inutile de souligner que certains firewalls de la dernière génération intègrent dans leurs fonctionnalités, la détection d'attaques ou d'intrusions. Mais il convient, avant de les acheter sur le marché, de bien vérifier si ces

[43] Frolick (M. N.), op. cit.
[44] Wang (W.) *« Hackers. Les secrets »*. Editions Micro Applications, Paris, 2003, p.312.
[45] Royer (J.- M.), op. cit., p.140.
[46] O'Connell (T.) *« Cyber soldiers »*, Security. March 1999.

fonctionnalités sont réellement incorporées à ces outils de défense et de protection des réseaux en informatique.

Somme toute, les systèmes englobant le matériel et les logiciels informatiques correctement mis en place et soigneusement bien entretenus, créent une solide base, propice à une sécurité efficace. Cependant, l'utilisation humaine de ces systèmes peut introduire des incertitudes et des erreurs. En plus des mesures technologiques prises pour protéger les ressources d'une organisation, une politique de sécurité informatique devrait être amorcée.

2.5. UNE POLITIQUE GLOBALE DE SECURITE

Cette politique de sécurité informatique doit d'abord être pensée, modulée et appliquée, en fonction de l'architecture de l'organisation considérée, en liaison avec tout réseau extérieur (comme le Web). Si la politique interne de sécurité de l'organisation n'a pas été, dans son format initial, conçue en prévision d'une connexion du réseau informatique interne avec un réseau externe, alors cela peut demander une modification de politique[47]. De ce fait, la politique interne de sécurité informatique de l'organisation doit être conséquemment améliorée et complétée par une autre composante de philosophie de sécurité. Celle-ci est alors imposée par la mise en place de la connexion à un réseau externe (comme le Web). Et à ce titre, la question principale peut être quels sont les niveaux supplémentaires de risques ou de vulnérabilité du réseau, qui seront introduits avec la réalisation du réseau proposé ? En tenant compte de cette interrogation, il est permis de penser à l'erreur humaine, qui constitue à nos yeux, un facteur essentiel à ne pas négliger, en matière de politique de sécurité informatique.

La politique de sécurité pourrait viser à protéger le système d'information d'une organisation en évitant l'introduction de l'erreur humaine. Généralement, dans une organisation, l'homme intervient à tous les niveaux, de la conception, de la construction et de l'exploitation de systèmes simples ou complexes. Cette intervention humaine peut être effectuée par un opérateur individuel, une équipe (groupe d'individus) ou le management (encadrement). Tous ces intervenants sont en interaction. Et les erreurs humaines peuvent se produire à n'importe quel moment du cycle de vie d'un système donné. Il est plus rentable et efficace de les anticiper lors de la phase de conception, puis, de mettre en œuvre, les parades requises[48]. C'est dans cette optique que se situe le développement suivant, consacré à une politique globale de sécurité informatique. Celle-ci concerne à la fois, le matériel et les logiciels informatiques d'une organisation. Il est opportun de préciser que, virtuellement chaque adresse IP accessible sur l'Internet, est régulièrement scrutée par des pirates informatiques.[49]
Le seul moyen de s'assurer qu'une organisation en réseau soit sûre est de supposer, qu'à tout moment, son système d'information puisse être attaqué, de n'importe où[50].
Les organisations commettent, communément, un certain nombre d'inadvertances qui compromettent leur sécurité informatique. Il n'est pas inutile de mentionner quelques unes[51] :

- mettre en place a posteriori, la sécurité comme solution à un système préalablement défaillant ;

[47] Maier (P. Q.) « *Insuring extranet security and performance* », Information Systems Management, Spring 2000, p.34-35.
[48] Leroy (A.) et Signoret (J.-P.) *« Le risque technologique »* Editions Presses universitaires de France (PUF) – Que sais-je. Paris 1992, p.99.
[49] Heiser (J.) *« Good offense is best defense against back origine »* Network World. August 9 1999.
[50] Noonan (T.) *« Beware the three network security myths »*. Computing Canada. November 26 1999.
[51] Dunlap (C.) *« Hachers for hire »*. Computer Reseller News. February 14 2000.

- ne pas avoir une philosophie de sécurité commune à tous les départements de l'organisation ;
- mélanger les composantes de matériel et logiciels, de telle manière que des éléments tels que les routeurs et les firewalls ne se trouvent pas synchronisés entre eux.

En anticipant la survenance des risques et attaques informatiques, il faudrait concevoir et mettre en place, au sein de l'organisation une philosophie de sécurité informatique, comme un ensemble homogène. Pour cela, il faudrait qu'un cadre au moins, ait une vision globale du réseau informatique et de sa sécurité[52]. On conçoit que la politique de sécurité devra émaner de l'encadrement (management) et non du personnel dévolu aux tâches opérationnelles. Cependant, la connaissance et la compréhension, par les utilisateurs, des recommandations de la politique de sécurité sont fondamentales pour l'application de celle-ci. Il est clair qu'à cette condition, les investissements relatifs à la mise en œuvre d'une politique de sécurité auront une utilité[53].

Somme toute, sur la base de notre expérience professionnelles, nous pouvons souligner que certaines organisations, souvent de taille moyenne, appartement à plusieurs branches d'activités, s'opposent, volontairement, à toute politique ou à toute mise en place de moyens de sécurité informatique. Les dirigeants de ces organisations justifient cette forme d'insouciance, en mettant en avant, le coût financier dit « élevé » de la sécurité informatique. Et ces dirigeants déclarent ne pouvoir changer d'avis que lorsqu'une attaque ou un sinistre se produira dans leur système d'information. Au-delà de cette prise de position relevant de l'incurie de certains dirigeants, il faut considérer que la sécurité, dans une organisation, doit être une préoccupation constante. Et il est souhaitable, que le schéma global de la sécurité soit construit au moment de la mise en place d'un système d'information (et non, après la survenance d'une attaque). A travers un plan harmonieux, le schéma de la sécurité du matériel informatique peut être mieux coordonné. Il va de soi, que pour une organisation, disposer d'une norme commune de sécurité entre les départements est aussi important. De ce fait, une approche de la sécurité informatique sur plusieurs fronts, semble constituer le meilleur moyen de mettre sur pied ce schéma. A ce titre, un ensemble de procédures (instructions écrites) normées écarterait une bonne part de risques. Se disant, nous pouvons évoquer les principaux points suivants :

- ne permettre aux utilisateurs d'accéder qu'à ce dont ils ont besoin. Car, un utilisateur mécontent ne peut détruire ce à quoi il ne peut accéder;
- former les utilisateurs à ne pas ouvrir des logiciels envoyés par courrier électronique (courriel) même si cela provient d'une source fiable. Cette discipline est destinée à éviter le plus possible, les codes malveillants ;
- orienter les utilisateurs vers une sélection rationalisée des mots de passe, et mettre en place, une politique de mots de passe et de codes ;
- installer un antivirus sur tous les ordinateurs de bureau et le configurer pour donner à l'organisation, une meilleure chance de détruire les attaques.

Au demeurant, d'autres procédures et moyens peuvent fournir à une organisation, une protection correcte. On pense ici, aux sauvegardes optimisées des données informatiques, à l'utilisation de salle blanche, à la biométrie,…Cependant, ces démarches doivent être en place et doivent être une composante d'un système de sécurité plus élargi. La sécurité relative au Web mise en œuvre sur le plan interne des organisations devient coûteuse pour celles-ci. Le personnel de sécurité correctement entraîné et expérimenté est cher et dans certains domaines,

[52] Muller (P. E.) et Fontaine (P.) *« Sécurisez votre réseau »*. Editions Micro Application. Paris 2004, p.46
[53] Léopold (E.) et Lhoste (S.) *« La sécurité informatique »*. Editions PUF, Que sais- je. Paris, 1999, p.124.

il est rare ou indisponible. Les petites et les grandes organisations commencent par sous-traiter leur fonction de sécurité à des fournisseurs de service de sécurité contrôlé-en anglais cela s'appelle Managed Security Service Provider (MSSP). L'offre de ces MSSP s'étend sur une gamme de services : la gestion de firewalls, l'examen de la vulnérabilité des VPN, la détection des intrusions, le contrôle et la gestion en temps réel[54]. Les MSSP peuvent, non seulement, contrôler et gérer continuellement les systèmes d'information des organisations, au niveau de la violation de leur sécurité, mais aussi connaître les nouvelles menaces et attaques qui sont en constante augmentation. Par exemple, nous pouvons rappeler que, durant le seul mois d'avril 2004, il a été détecté plus 1400 nouveaux codes malins sur l'Internet[55]. Conscientes de ces dangers, ces MSSP pourront prendre des mesures préventives, destinées à éviter des attaques. Somme toute, afin de préserver certaines informations sensibles sur le plan interne, certaines organisations acceptent de sous-traiter une portion de leur fonction de sécurité à ces MSSP, au lieu de leur en confier la totalité.

En regardant l'avenir et non le passé, on reconnaîtra que le « grid computing » présente des promesses pour les systèmes d'information en réseaux. Actuellement, le « grid computing », constitue une technologie qui s'applique essentiellement dans l'informatique scientifique et universitaire. Il permet à des programmes demandant d'importantes capacités de calculs, de s'appuyer sur une myriade d'ordinateurs reliés entre eux, par des réseaux locaux étendus[56]. Avec le « grid », il ne sera plus nécessaire de décider à l'avance, quelle application sera réalisée pour tourner sur tel serveur. Les ressources étant mobilisées dynamiquement, en fonction des besoins informatiques du moment. Il est satisfaisant de savoir que ce concept commence par s'introduire dans le monde commercial et dans l'informatique de gestion. A ce titre, la nouvelle base de données de l'éditeur de logiciels ORACLE, dénommée « 10 g[57] », est la réponse fournie aux firmes voulant mieux utiliser leurs ressources informatiques. Ce modèle est appelé à révolutionner toute l'infrastructure informatique des entreprises. On peut espérer que cette évolution ne compliquera pas la sécurisation des systèmes informatiques des organisations en réseaux, adoptant le « grid computing ».

CONCLUSION

De nos jours, l'utilisation des ordinateurs soulève des problèmes de sécurité. Dans cet article, nous avons fourni les principaux outils et politiques, indispensables pour conférer aux réseaux des systèmes d'information de gestion, un excellent niveau de sécurisation contre les attaques externes, émanant des pirates informatiques et contre les dangers potentiels, voulus et prémédités ou non, initiés à l'intérieur des organisations. A ce titre, la sécurisation de site et de serveur Web a été l'objet d'une attention particulière. Par ailleurs, nous avons mis l'accent sur l'obligation pour une organisation, de mettre sur pied et d'appliquer une rigoureuse politique de sécurité informatique. Mais pour cette sécurisation, c'est le statut important accordé à ses déclinaisons, aux firewalls et aux réseaux privés virtuel (VPN), qui nous a

[54] En France, de plus en plus de fournisseurs d'accès à l'Internet se portent offreurs de services sur ce créneau de la sécurité informatique, concurrençant de ce fait, les sociétés spécialisées dans la sécurité informatique pure.
[55] Foucart (S.), op. cit.
[56] A l'Institut national de la recherche en informatique et automatique (INRIA), à Grenoble, on définit le « grid computing » comme une technologie permettant de relier un ensemble de grappes d'ordinateurs (« clusters ») par l'intermédiaire d'un réseau longue distance.
[57] Où le g désigne grid c'est-à-dire grille en français. Voir Abramson (I.), Abbey (M.) et Corey (M.) « *Oracle database 10 g. A beginner's guide* ». Editions The McGraw-Hill, Inc. Traduction française. *« Oracle 10 g. Notion fondamentales »*. Editions CampusPress. Paris 2004, p.27.

semblé être le plus important, pour donner à une organisation, une grande chance de sécuriser les réseaux de son système d'information.

En scrutant l'avenir, on remarquera que l'utilisation abondante et la multiplication exponentielle des ordinateurs dans le monde, pourront poser, dans le futur, des problèmes relatifs à la sécurité et à la qualité de l'environnement, en général. Et ceci concerne déjà les ordinateurs usagés. En effet, des centaines de millions d'ordinateurs et de déchets électriques et électroniques en provenance du monde entier et surtout des Etats-Unis, d'Europe, d'Asie, sont transportés par conteneurs entiers, et envoyés en Chine, en Inde et au Pakistan. Dans ce dernier pays, on peut attirer l'attention du lecteur sur la décharge de Shershah, à Karachi, où ces ordinateurs et d'autres déchets électroniques sont expédiés à la casse[58]. Concernant les ordinateurs à proprement parler, si une partie de ces appareils se trouve réparée, remontée et revendue, sur le marché local, une autre partie plus importante, livre ses composantes à la destruction, à la combustion et à la récupération. Pour pouvoir récupérer les métaux, les cartes graphiques et les processeurs, il convient d'abord, de les chauffer et même de les brûler. Et ce processus s'accompli souvent sans aucune protection contre ces fumées nauséabondes et cancérigènes. C'est dangereux car un ordinateur est truffé de matériel toxiques, de substances chlorées, bromées, de métaux lourds (plombs, oxyde de plomb, cadmium, baryum,… et mercure) ainsi que de produits plastiques. Ces composantes de l'ordinateur produisent, au cours de leur combustion, des dioxines et du furanne.

Selon l'institut états-unien Dataquest, plus d'un milliard d'ordinateurs auraient, depuis 1975, déjà été vendus sur le marché[59]. Or ces appareils sont soumis à une obsolescence de plus en plus rapide qui accélère le renouvellement du parc informatique. Il n'est pas inadéquat, de signaler que le nombre de déchets électroniques est en croissance forte en Europe et aux Etats-Unis. Ces déchets surnommés « e déchets », sont exportés comme nous venons de le dire surtout au Pakistan, en Chine et en Inde, à des fins dites de recyclage.

Nous pensons, pour notre part, qu'à long terme, si ce phénomène se poursuit, cela risque de porter préjudice à l'environnement mondial. Le recyclage des ordinateurs usagés créera, de notre point de vue, dans le futur, un vrai et grave problème de sécurité et de société au regard de l'environnement. On comprendra alors, qu'au défi de la sécurisation des réseaux informatiques de gestion, s'ajoutera désormais, dans un proche avenir, le défi de la sécurité de l'environnement, engendré par l'explosion d' « e déchets ».

REFERENCES

Abbey (M.), Abramson (I.) et Corey (M.) "*Oracle database 10g. A beginner's guide*". Editions The McGraw-Hill, Inc. Traduction française. « *Oracle 10g. Notions fondamentales* ». Editions CampusPress. Paris 2004, p. 27.

Abramson (I.), Abbey (M.) et Corey (M.) "*Oracle database 10g. A beginner's guide*". Editions The McGraw-Hill, Inc. Traduction française. « *Oracle 10g. Notions fondamentales* ». Editions CampusPress. Paris 2004, p. 27.

Anonyme, voir *« Firewall Guard Perimeter »,* Security. June 1999.

Balle (F.) et Cohen -Tanugi (L.) « *Dictionnaire du Web* ». Edition Dalloz, Paris 2001, p.296-297.

Camborde (C.), *« Sécuriser vos applications Internet* ». Editions Dunod, Paris, p. 92

[58] Draper (A.*) « L'électronique se décharge à Karachi »,* Libération du 18 août 2004, p. 08.
[59] Idem.

Cohen -Tanugi (L.) et Balle (F.) « *Dictionnaire du Web* ». Edition Dalloz, Paris 2001, p.296-297.
Corey (M.) Abbey (M.) et Abramson (I.) "*Oracle database 10g. A beginner's guide*". Editions The McGraw-Hill, Inc. Traduction française. « *Oracle 10g. Notions fondamentales* ». Editions CampusPress. Paris 2004, p. 27.
Corvalan (E.), Corvalan (R.) et Le Corvic (Y.), *« Les VPN : principes, conception et déploiements des réseaux privés virtuels »*. Editions Dunod, Paris 2003, p. 24.
Corvalan (R.), Corvalan (E.) et Le Corvic (Y.), *« Les VPN : principes, conception et déploiements des réseaux privés virtuels »*. Editions Dunod, Paris 2003, p. 24.
Draper (A.*) « L'électronique se décharge à Karachi »*, Libération du 18 août, 2004, p. 08.
Dunlap (C.) *« Hachers for hire »*. Computer Reseller News. February 14, 2000.
Durant (J.) et Maussion (C.) *« Bracage de banque sur le Net »*, Libération du 20 août 2004, p. 12
Elsbery (R. B.) *« The Spying game : how safe are your secrets ? »*, Office Systems. September 1999.
Finez (L.) *« Sécurité informatique »*, Magazine FACE, Chambre de commerce et d'industrie de Lille (France). Févvier 2003, p. 29.
Fontaine (P.) et Muller (P. E.) *« Sécurisez votre réseau »*. Editions Micro Application. Paris 2004, p. 46.
Foucart (S.) *« Les créateurs de virus informatiques deviennent des mercenaires »*, le Monde du 28 avril 2004, p. 24
Franson (P.), *« Thwarting hackers »*, Electronic Business. May 2000.
Frolick (M. N.) *« A new master's guide to firewalls and security »*, Information Systems Management. Winter 2003, p. 29-33.
Gips (M. A.) *« Is your site a hacker's delight ? »*, Security Management. August 1999.
Golman (J. E.) *« Applied Data Communications. A business Oriented Approach »*, Wiley 1998.
Heiser (J.) *« Good offense is best defense against back origine »* Network World. August 9, 1999.
Higgins (K. J.) *« Human element is key to stoppping hackers »*, Information Week. May 29 2000.
Janss (S.) *«Frontier defense : personnal firewalls software »*, Network World. August 7 2000.
Keong (V.) *« The Ethical hack »*, C. A. Magazine. January/February 2000.
Kuipers (F.) *« Preventing the Hack Attack »*, Telecommunication. July 2000.
Le Corvic (Y.), Corvalan (E.) et Corvalan (R.) *« Les VPN : principes, conception et déploiements des réseaux privés virtuels »*. Editions Dunod, Paris 2003, p. 24.
Léopold (E.) et Lhoste (S.) *« La sécurité informatique »*. Editions PUF, Que sais- je. Paris, 1999, p. 124.
Leroy (A.) et Signoret (J.-P.) *« Le risque technologique »*. Editions Presses universitaires de France (PUF) – Que sais-je. Paris 1992, p. 99.
Lhoste (S.) et Léopold (E.) *« La sécurité informatique »*. Editions PUF, Que sais- je. Paris, 1999, p. 124.
Maier (P. Q.) « *Insuring extranet security and performance »*, Information Systems Management, Spring 2000, p. 34-35.
Males (D.), Pujolle (G.) *« WI-FI par la pratique »*. Editions Eyrolles, Paris 2004, p. 119. et p. 134-135
Maussion (C.) *« Bracage de banque sur le Net »*, Libération du 20 août 2004, p. 12.
Messmer (E.) *« Second line of defense »*, Network World. July 2000.

Muller (P. E.) et Fontaine (P.) *« Sécurisez votre réseau »*. Editions Micro Application. Paris 2004, p. 46.
Noonan (T.) *« Beware the three network security myths »*. Computing Canada. November 26, 1999.
O'Connell (T.) *« Cyber soldiers »*, Security. March 1999.
Plouin (G.) Soyer (J.), Triouller (M. E.) *« Sécurité des architectures Web »*. Editions Dunod, Paris 2004, p. 280-281
Pritchard (S.) *« Dealing with the threat from within »*, Financial Times. March 17 2004, p 04. Supplément I T Review
Pujolle (G.) et Males (D.), *« WI-FI par la pratique »*. Editions Eyrolles, Paris 2004, p. 119. et p. 134-135.
Royer (J.-M.), *« Sécuriser l'informatique de l'entreprise : enjeux, menaces, prévention et parades »*. Edition ENI, Nantes 2004, p. 53.
Shillingford (J.) *« Push-to-talk services gain ground »*, Financial Times. March 17 2004, p 04. Supplément I T Review.
Signoret (J.-P.) et Leroy (A.) *« Le risque technologique »*. Editions Presses universitaires de France (PUF) – Que sais-je. Paris 1992, p. 99.
Soyer (J.), Plouin (G.) et Triouller (M. E.) *« Sécurité des architectures Web »*. Editions Dunod, Paris 2004, p. 280-281
Taylor (P.) *« Keep out my inbox »*, Financial Times. March 17 2004, p 04. Supplément I T Review p. 08.
Triouller (M. E.), Soyer (J.) et Plouin (G.) *« Sécurité des architectures Web »*. Editions Dunod, Paris 2004, p. 280-281
Wang (W.) *« Hackers. Les secrets »*. Editions Micro Applications, Paris, 2003, p. 312.