LA SÉCURITÉ INFORMATIQUE

1 PRINCIPES DE LA SÉCURITÉ

1.1 Exigences fondamentales

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité :

1. **disponibilité :** demande que l'information sur le système soit *disponible* aux personnes autorisées.
2. **Confidentialité :** demande que l'information sur le système ne puisse être *lue* que par les personnes autorisées.
3. **Intégrité :** demande que l'information sur le système ne puisse être *modifiée* que par les personnes autorisées.

La sécurité recouvre ainsi plusieurs aspects :

- intégrité des informations (pas de modification ni destruction)
- confidentialité (pas de divulgation à des tiers non autorisés)
- authentification des interlocuteurs (signature)
- respect de la vie privée (informatique et liberté).

Du point de vue de la sécurité informatique, une menace est une violation potentielle de la sécurité. Cette menace peut-être accidentelle, intentionnelle (attaque), active ou passive.

1.2 Étude des risques

Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi. Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés. L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque. On obtient ainsi la liste de ce qui doit être protégé.

Il faut cependant prendre conscience que les principaux risques restent : « câble arraché », « coupure secteur », « crash disque », « mauvais profil utilisateur », « test du dernier CD Bonux »…

Voici quelques éléments pouvant servir de base à une étude de risque:

- Quelle est la valeur des équipements, des logiciels et surtout des informations ?
- Quel est le coût et le délai de remplacement ?
- Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau (programmes d'analyse des paquets, logs…).
- Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société ?

1.3 Établissement d'une politique de sécurité

Suite à l'étude des risques et avant de mettre en place des mécanismes de protection, il faut préparer une politique à l'égard de la sécurité. C'est elle qui fixe les principaux paramètres, notamment les niveaux de tolérance et les coûts acceptable. Voici quelques éléments pouvant aider à définir une politique :

- Quels furent les coûts des incidents informatiques passés ?
- Quel degré de confiance pouvez vous avoir envers vos utilisateurs interne ?
- Qu'est-ce que les clients et les utilisateurs espèrent de la sécurité ?
- Quel sera l'impact sur la clientèle si la sécurité est insuffisante, ou tellement forte qu'elle devient contraignante ?
- Y a-t-il des informations importantes sur des ordinateurs en réseaux ? Sont-ils accessible de l'externe ?
- Quelle est la configuration du réseau et y a-t-il des services accessibles de l'extérieur ?
- Quelles sont les règles juridiques applicables à votre entreprise concernant la sécurité et la confidentialité des informations (ex: loi « informatique et liberté », archives comptables…) ?

1.4 Éléments d'une politique de sécurité

Il ne faut pas perdre de vue que la sécurité est comme une chaîne, guère plus solide que son maillon le plus faible. En plus de la formation et de la sensibilisation permanente des utilisateurs, la politique de sécurité peut être découpée en plusieurs parties :

- **Défaillance matérielle :** Tout équipement physique est sujet à défaillance (usure, vieillissement, défaut…) L'achat d'équipements de qualité et standard accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction. Seule une forme de sauvegarde peut cependant protéger les données.
- **Défaillance logicielle :** Tout programme informatique contient des bugs. La seule façon de se protéger efficacement contre ceux-ci est de faire des copies de l'information à risque. Une mise à jour régulière des logiciels et la visite des sites consacrés à ce type de problèmes peut contribuer à en diminuer la fréquence.
- **Accidents (pannes, incendies, inondations…) :** Une sauvegarde est indispensable pour protéger efficacement les données contre ces problèmes. Cette procédure de sauvegarde peut combiner plusieurs moyens fonctionnant à des échelles de temps différentes :
  - disques RAID pour maintenir la disponibilité des serveurs.
  - copie de sécurité via le réseau (quotidienne)
  - copie de sécurité dans un autre bâtiment (hebdomadaire)

  La disposition et l'infrastructure des locaux peut aussi fournir une protection intéressante.

  Pour des sites particulièrement important (site informatique central d'une banque…) il sera nécessaire de prévoir la possibilité de basculer totalement et rapidement vers un site de secours (éventuellement assuré par un sous-traitant spécialisé). Ce site devra donc contenir une copie de tous les logiciels et matériels spécifiques à l'activité de la société.
- **Erreur humaine :** Outre les copies de sécurité, seule une formation adéquate du personnel peut limiter ce problème.
- **Vol via des dispositifs physique (disques et bandes) :** Contrôler l'accès à ces équipements : ne mettre des unités de disquette, bandes… que sur les ordinateurs où c'est essentiel. Mettre en place des dispositifs de surveillances.
- **Virus provenant de disquettes :** Ce risque peut-être réduit en limitant le nombre de lecteur de disquettes en service. L'installation de programmes antivirus peut s'avérer une protection efficace mais elle est coûteuse, diminue la productivité, et nécessite de fréquentes mises à jour.
- **Piratage et virus réseau :** Cette problématique est plus complexe et l'omniprésence des réseaux, notamment l'Internet, lui confère une importance particulière. Les problèmes

de sécurité de cette catégorie sont particulièrement dommageables et font l'objet de l'étude qui suit.

1.5 Principaux défauts de sécurité

Les défauts de sécurité d'un système d'information les plus souvent constatés sont :

- Installation des logiciels et matériels par défaut.
- Mises à jours non effectuées.
- Mots de passe inexistants ou par défaut.
- Services inutiles conservés (Netbios…).
- Traces inexploitées.
- Pas de séparation des flux opérationnels des flux d'administration des systèmes.
- Procédures de sécurité obsolètes.
- Eléments et outils de test laissés en place dans les configurations en production.
- Authentification faible.
- Télémaintenance sans contrôle fort.

1.6 Éléments de droits

Intrusions informatiques : loi « Godfrain » du 5/1/88

Art. 323-1. Le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30 000 € d'amende.

Art. 323-2. Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 € d'amende.

Art. 323-3. Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, ou de supprimer ou de modifier frauduleusement des données qu'il contient est puni de trois ans d'emprisonnement et de 45 000 € d'amende.

Loi 78/17 du 6/01/78 relative à l'informatique, aux fichiers et aux libertés

Article 29 Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes les précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

Voir aussi la **Directive 95/46/CE du 24 octobre 1995** article 17 (sécurité des traitements)

LSQ (Loi sur la Sécurité Quotidienne) dont on attend les décrets…

2 FAILLES DE SÉCURITÉ SUR INTERNET

En entreprise, c'est le réseau local qui est connecté à Internet. Il est donc indispensable de contrôler les communications entre le réseau interne et l'extérieur. De plus une formation du personnel est indispensable (règles de sécurité, déontologie, attention aux participations aux forums qui sont archivées ...).

Les problèmes de sécurité qu'on peut rencontrer sur un réseau d'entreprise ou sur l'Internet relèvent d'abord de la responsabilité des victimes avant d'être imputables aux hackers. Une menace qui a sensiblement augmenté au cours de ces dernières années, nous indique la dernière étude du *Computer Security Institute*, un institut professionnel de San Francisco qui réalise chaque année un sondage auprès des entreprises en collaboration avec le FBI. Dans cette étude, plus de 40 % des sociétés interrogées ont déclaré que des intrus s'étaient introduits dans leurs systèmes depuis l'Internet, 38 % des sociétés ont détecté des attaques de type "déni de service", et 94 % ont été infectées par un virus en 2000.

D'autre part, votre sécurité peut dépendre d'autres entreprises dont vous pensez, parfois à tort, qu'elles ont assuré leur propre sécurité. Alors que le gouvernement et les forces de l'ordre cherchent à interpeller les intrus, les sociétés ne se préoccupent trop souvent que de relancer leurs réseaux après une attaque. « Le secteur privé ne cherche pas à savoir qui est responsable, tout ce qui intéresse les entreprises, c'est que l'attaque cesse. ».

2.1 Définitions

2.1.1 IP spoofing

Usurpation d'adresse IP, on fait croire que la requête provient d'une machine autorisée. Une bonne configuration du routeur d'entrée permet d'éviter qu'une machine extérieure puisse se faire passer pour une machine interne.

2.1.2 DNS spoofing

Pousse un serveur de DNS à accepter l'intrus. Solution : séparer le DNS du LAN de celui de l'espace public.

2.1.3 Flooding

Raid massif de connexions non terminées.

2.1.4 smurf

Saturation de la bande passante.

2.1.5 Web bug

Un mail publicitaire est envoyé en HTML (même si l'apparence est normale) avec une image transparente gif d'un pixel par un lien du type :

<img src="http://www.serveur.xx/image.gif ?email=utilisateur@adresse">

Si le courrier est ouvert pendant la connexion, la requête de téléchargement de l'image vient confirmer la lecture du message et la validité de votre adresse.

Conseil : ne pas valider l'ouverture automatique du format HTML ou ne pas ouvrir ses courriers en ligne. Un utilitaire de détection de « web bug » BUGNOSIS est disponible sur ***www.bugnosis.org*** .

2.1.6 Hoax (rumeur)

Un « hoax » est une rumeur que l'on transmet par mail. Ces rumeurs colportent souvent des problèmes de sécurité soit disant découverts par des services officiels ou célèbres… Elles peuvent causer un véritable préjudice à certaines sociétés et de toute façon encombrent le réseau. Avant de retransmettre un tel message il est prudent de vérifier son authenticité. ***www.hoaxbuster.com*** (site français) recense la plupart des messages bidons.

2.1.7 Hacker et cracker

Il existe une communauté, une culture partagée, de programmeurs expérimentés et de spécialistes des réseaux, dont l'histoire remonte aux premiers mini-ordinateurs multi-utilisateurs, il y a quelques dizaines d'années, et aux premières expériences de l'ARPAnet. Les membres de cette culture ont créé le mot ***"hacker"***. Ces informaticiens sont généralement discrets, anti-autoritaristes et motivés par la curiosité.

Il y a un autre groupe de personnes qui s'autoproclament des "hackers". Ces gens (principalement des adolescents de sexe masculin) prennent leur pied en s'introduisant à distance dans les systèmes informatiques et en piratant les systèmes téléphoniques, généralement à l'aide d'outils écrit par d'autres et trouvés sur Internet. Ils publient sur alt.2600. Les vrais hackers appellent ces gens des ***"crackers"*** et ne veulent rien avoir à faire avec eux. Les vrais hackers pensent que les crackers sont des gens *paresseux, irresponsables et pas très brillants*.

2.2 Principales attaques

2.2.1 Virus

Les virus est un exécutable qui va exécuter des opérations plus ou moins destructrices sur votre machine. Les virus existent depuis que l'informatique est née et se propageaient initialement par disquettes de jeux ou logiciels divers... Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

- Téléchargement de logiciel puis exécution de celui-ci sans précautions,
- Ouverture sans précautions de documents contenant des macros,
- Pièce jointe de courrier électronique (exécutable, script type vbs…),
- Ouverture d'un courrier au format HTML contenant du javascript exploitant une faille de sécurité du logiciel de courrier (normalement javascript est sans danger).
- Exploitation d'un bug du logiciel de courrier (effectuer régulièrement les mises à jour).

Les virus peuvent être très virulent mais ils coûtent aussi beaucoup de temps en mise en place d'antivirus et dans la réparation des dégâts causés. On peut malheureusement trouver facilement des logiciels capables de générer des virus et donc permettant à des « amateurs » (aussi appelés *crackers*) d'étaler leur incompétence.

La meilleure parade est l'utilisation d'un antivirus à jour et d'effectuer les mises à jour des logiciels (pour éviter l'exploitation des bugs).

2.2.2 Déni de service (DoS)

Le but d'une telle attaque n'est pas de dérober des informations sur une machine distante, mais de paralyser un service ou un réseau complet. Les utilisateurs ne peuvent plus alors accéder aux ressources. Les deux exemples principaux, sont le « ping flood » ou

l'envoi massif de courrier électroniques pour saturer une boîte aux lettre *(mailbombing).* La meilleure parade est le firewall ou la répartition des serveurs sur un réseau sécurisé.

2.2.3 Écoute du réseau (sniffer)

Il existe des logiciels qui, à l'image des analyseurs de réseau, permettent d'intercepter certaines informations qui transitent sur un réseau local, en retranscrivant les trames dans un format plus lisible *(Network packet sniffing).* C'est l'une des raisons qui font que la topologie en étoile autour d'un hub n'est pas la plus sécurisée, puisque les trames qui sont émises en « broadcast » sur le réseau local peuvent être interceptées. De plus, l'utilisateur n'a aucun moyen de savoir qu'un pirate a mis son réseau en écoute.

L'utilisation de *switches* (commutateurs) réduit les possibilités d'écoute mais en inondant le commutateur, celui-ci peut se mettre en mode « HUB » par « sécurité » !

La meilleure parade est l'utilisation de mot de passe non rejouable, de carte à puce ou de calculette à mot de passe.

2.2.4 Intrusion

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace et est donc une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, incident diplomatique, chantage…

Le principal moyen pour prévenir les intrusions est le coupe-feu ("firewall"). Il est efficace contre les fréquentes attaques de pirates amateurs, mais d'une efficacité toute relative contre des pirates expérimentés et bien informés. Une politique de gestion efficace des accès, des mots de passe et l'étude des fichiers « log » (traces) est complémentaire.

2.2.5 Cheval de Troie

L'image retenue de la mythologie est parlante; le pirate, après avoir accédé à votre système ou en utilisant votre crédulité, installe un logiciel qui va, à votre insu, lui transmettre par Internet les informations de vos disques durs. Un tel logiciel, aussi appelé troyen ou *trojan*, peut aussi être utilisé pour générer de nouvelles attaques sur d'autres serveurs en passant par le votre. Certains d'entre eux sont des « key logger » c'est à dire qu'ils enregistrent les frappes faites au clavier.

La première mesure de protection face aux attaques, et de sécuriser au maximum l'accès à votre machine et de mettre en service un antivirus régulièrement mis à jour. Un nettoyeur de troyens peut aussi s'avérer utile.

Attention : sous Windows, un partage de fichiers actif et trop permissif offre les mêmes possibilités sans que le visiteur n'ai besoin d'installer un logiciel !

2.2.6 « social engeneering »

En utilisant les moyens usuels (téléphone, email…) et en usurpant une identité, un pirate cherche à obtenir des renseignements confidentiels auprès du personnel de l'entreprise en vue d'une intrusion future. Seule une formation du personnel permet de se protéger de cette attaque.

2.3 ESPIONNAGE

2.3.1 L'homme du milieu

Lorsqu'un pirate, prenant le contrôle d'un équipement du réseau, se place au milieu d'une communication il peut écouter ou modifier celle-ci. On parle alors de « l'homme du milieu » *(man in the middle)*. Les point sensibles permettant cette technique sont :

- **DHCP** : ce protocole n'est pas sécurisé et un pirate peut fournir à une victimes des paramètres réseau qu'il contrôle. Solution : IP fixe.
- **ARP** : si le pirate est dans le même sous réseau que la victime et le serveur (même si commutateur), il peut envoyer régulièrement des paquets ARP signalant un changement d'adresse MAC aux deux extrémités. Solution : ARP statique.
- **ICMP** : Un routeur peut émettre un ICMP-redirect pour signaler un raccourci, le pirate peut alors demander de passer par lui. Solution : refuser ICMP-redirect ou seulement vers des routeurs identifiés.
- **RIP** : Le pirate envoie une table de routage à un routeur indiquant un chemin à moindre coût et passant par un routeur dont il a le contrôle. Solution : nouvelle version de RIP qui intègre une identification des routeurs de confiance.
- **DNS** : par « ID spoofing » un pirate peut répondre le premier à la requête de la victime et par « cache poisoning » il corrompt le cache d'un serveur DNS. Solution : proxy dans un réseau différent des clients, désactivation de la récursivité, vidage du cache DNS régulier.
- **Proxy HTTP** : Par définition un proxy est en situation d'homme du milieu. Une confiance dans son administrateur est nécessaire de même qu'un contrôle du proxy lors de son départ !
- **Virus** : un virus, éventuellement spécifique à la victime et donc indétectable, peut écrire dans le fichier « hosts »… Solution : bloquer les .vbs et .exe

2.3.2 Espiogiciels

Ces logiciels espions sont aussi appelés ***« spyware ».*** Ils ne posent pas, à priori, de problème de sécurité mais plutôt celui du respect de la vie privée.

Plusieurs logiciels connus se permettent de renvoyer vers l'éditeur des informations concernant l'usage du logiciel mais aussi sur les habitudes ou la configuration de l'utilisateur, et ceci au mépris de la loi « informatique et liberté ». Il s'agit souvent de « freewares » qui trouvent ainsi une source de revenus mais pas toujours !

Exemples : Real Networks (requête vers l'éditeur à chaque insertion de CD-audio avec n° GUID, adresse mail…), CuteFTP…

Une liste des programmes suspects et un outil gratuit (**Ad-Aware**) est disponible sur ***www.lavasoft.com*** .

Logiciel pour supprimer des espions recensés : optout.exe sur ***//grc.com***

2.3.3 Cookies

Un « cookies » est une chaîne de caractère qu'un serveur dépose sur votre disque dur, via votre navigateur, afin normalement d'accélérer ou d'autoriser votre prochaine visite. On trouvera des infos sur les cookies à ***www.epic.org/privacy/internet/cookies***

Des logiciels permettant le tri des cookies sont disponibles : « cookie crusher » sur ***www.thelimitsoft.com*** et « cache & cookiewasher » sur ***www.webroot.com***

3 PROTECTIONS

3.1 FORMATION DES UTILISATEURS

On considère généralement que la majorité des problèmes de sécurité sont situés entre la chaise et le clavier ...! ;-)

Discrétion : la sensibilisation des utilisateurs à la faible sécurité des outils de communication et à l'importance de la non divulgation d'informations par ces moyens est indispensable. En effet il est souvent trop facile d'obtenir des mots de passe par téléphone ou par e-mail en se faisant passer pour un membre important de la société.

Virus : plusieurs études récentes (2001) montrent que 1/3 des utilisateurs ouvriraient encore une pièce jointe d'un courrier nommée « i love you » et que la moitié ouvriraient une pièce nommée « ouvrez-ça » ou similaire… ! L'information régulière du personnel est nécessaire, attention toutefois aux rumeurs (hoax).

Charte : l'intérêt principal d'une charte d'entreprise est d'obliger les employés à lire et signer un document précisant leurs droits et devoirs et par la même de leur faire prendre conscience de leur responsabilité individuelle.

3.2 POSTE DE TRAVAIL

Le poste de travail reste un maillon faible de la sécurité. Le projet TCPA *(Trusted Computing Platform Alliance)* a pour but d'améliorer sa sécurité en dotant le PC d'une puce dédiée à la sécurité. Elle sera chargée de vérifier l'intégrité du BIOS, du chargement de l'OS, de sauvegarder les clés et certificats (PKI) et connaîtra les protocoles de cryptage (RSA, DES…).

- Plusieurs carte mère possèdent un cavalier interdisant la reprogrammation du BIOS (flashage), vérifier et mettre en place ce cavalier sur tous les postes !
- Lecteur de disquette : Interdire le Boot disquette (BIOS) voire inhiber complètement le fonctionnement du lecteur.
- Lecteur de CD-ROM : les virus de Boot sont très rares sur CD, mais avec la généralisation des graveurs et la simplification des logiciels de gravure…
- Backup régulier et sécurisé des informations essentielles.
- Multi-boot : à éviter au maximum car la sécurité globale du poste est celle de l'OS le plus fragile et de plus il existe des logiciels permettant de lire sous un OS les autres partitions en ignorant alors les sécurités (exemple : lecture de fichiers NTFS sans tenir compte des droits).

3.3 ANTIVIRUS

Principale cause de désagrément en entreprise, les virus peuvent être combattus à plusieurs niveaux.

La plupart des antivirus sont basés sur l'analyse de signature des fichiers, la base des signatures doit donc être très régulièrement mise à jour sur le site de l'éditeur (des procédures automatiques sont généralement possibles).

Deux modes de protection :

- Généralisation de l'antivirus sur toutes les machines, il faut absolument prévoir une mise à jour automatique de tous les postes via le réseau.

- Mise en place d'un antivirus sur les points d'entrée/sortie de données du réseau après avoir parfaitement identifiés tous ces points. La rigueur de tout le personnel pour les procédures doit être acquise.

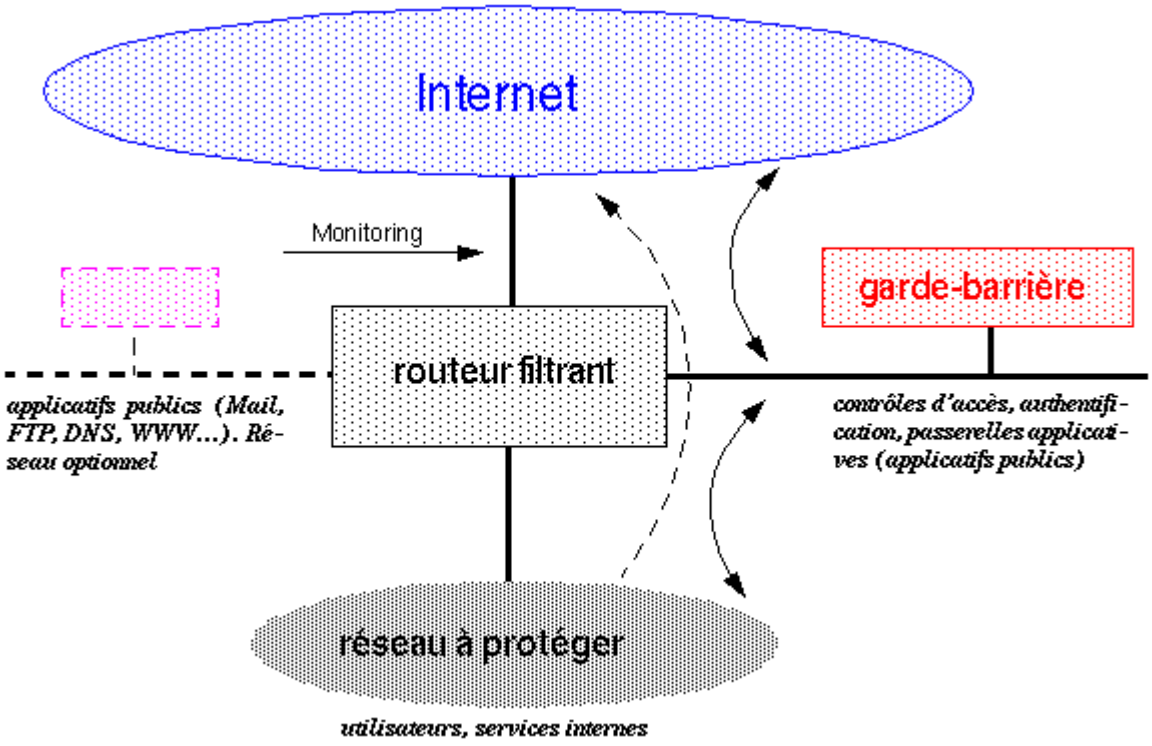
Messagerie : la plupart des virus actuels utilisent ce vecteur de transmission. Les vers s'installent et s'exécutent sans l'intervention de l'utilisateur (exécutable ouvert automatiquement, exploitation d'une faille du logiciel de messagerie…). La protection contre les virus en provenance de la messagerie doit être effectuée, non pas au niveau du poste de travail, mais du serveur. Ainsi certains antivirus agissent au niveau du coupe-feu, les deux outils coopérant via le protocole CVP *(Content Vectoring Protocol)* qui normalise leur communication. Les clients de messagerie de Microsoft sont victimes de leurs enrichissements en recourant à Word ou au HTML pour éditer le message, ils rendent possible l'exécution de macrovirus. La parade la plus simple consiste à n'utiliser ces clients de messagerie qu'en mode texte.

Attention, la mise en place d'un antivirus sur le firewall n'est d'aucun secours en cas de fichiers cryptés !

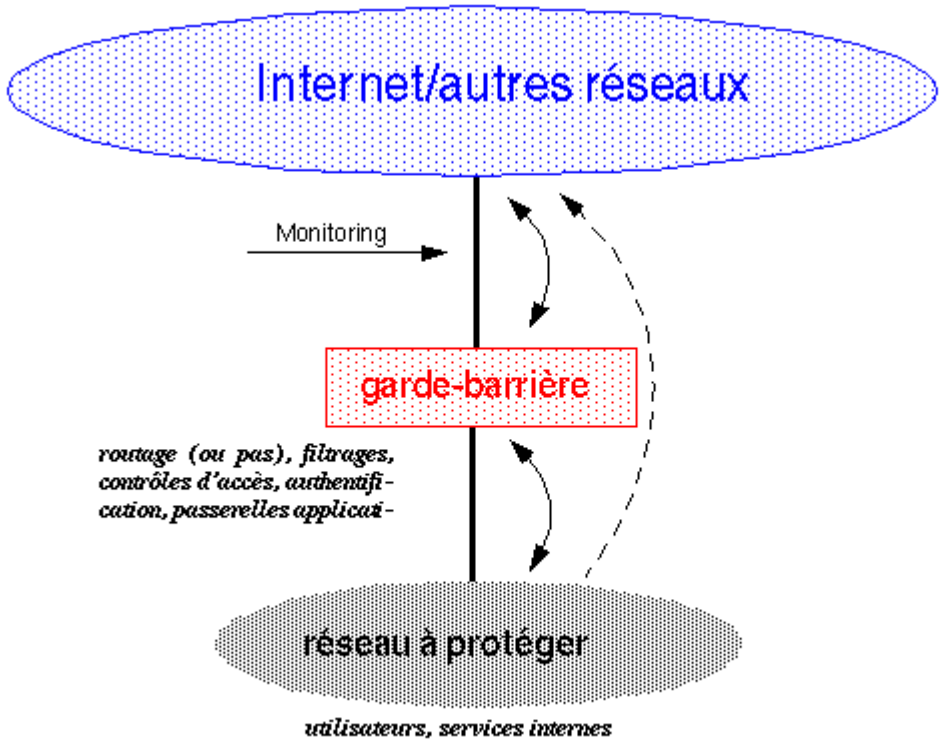
3.4 PARE-FEU (fire wall) ou GARDE BARRIÈRE

C'est une machine dédiée au routage entre LAN et Internet. Consulter la RFC2196. Le trafic est analysé au niveau des datagrammes IP (adresse, utilisateur, contenu...). Un datagramme non autorisé sera simplement détruit, IP sachant gérer la perte d'information. Une translation d'adresse pourra éventuellement être effectuée pour plus de sécurité (protocole NAT *Network Address Translation* RFC 1631+2663). Attention : un firewall est inefficace contre les attaques ou les bévues situées du coté intérieur et qui représentent 70% des problèmes de sécurité !

3.4.1 Architecture classique



3.4.2 Architecture concentrée



3.4.3 Logiciels

Par sécurité on désactivera tous les services inutiles (TELNET, ...) et on fermera tous les ports TCP/UDP inutilisés (ex TCP 139=Netbios pour partage de dossiers ! ...) (Un outil de protection personnel gratuit « zonealarm » est proposé par ***www.zonelabs.com*** ou bien « kerio personnal » chez ***www.kerio.com***) En logiciel libre on utilisera « Ipchain » (noyau Linux) ou « Netfilter » (similaire au produit de checkpoint). Pour ceux qui tournent sous MacOS, il en existe aussi quelques uns dont « Netbarrier » (intego.com) et « DoorStop » (opendoor.com).

Dans certains sites on place les serveurs liés aux services Internet dans une « zone démilitarisée » (DMZ), les accès en provenance d'Internet ne peuvent voir que ces machines et les utilisateurs de l'entreprise doivent passer par les machines de la DMZ pour accéder à Internet.

Au niveau réseau local, un programme correctement écrit (sniffer) peut quand même observer le trafic et saisir noms et mots de passe qui circuleraient sur le réseau à diffusion (Ethernet via Hubs) !

Dans le domaine commercial, les logiciels firewall les plus réputés sont VPN1 de checkpoint et e-trust de Computer Associates. Il existe aussi des boîtiers « tout compris » du type firebox de Watchguard ou Instagate de Techniland.

3.4.4 Filtrage de sites

Pour les écoles (protection des mineurs) ou bloquer les publicités… On peut télécharger un fichier répertoriant plusieurs milliers de serveurs sur ***www.accs-net.com/hosts***, un outils libre sur ce même site (eDeexer) permet de remplacer le carré blanc de la publicité manquante par l'image de son choix.

3.5 AUTHENTIFICATION ET CRYPTAGE

L'authentification est basée sur les 3 principes :

- **Savoir :** login, mot de passe…
- **Être :** biométrie (empreintes…)
- **Avoir :** clés USB, carte à puce, « token ».

Une authentification est dite forte lorsqu'elle utilise deux mécanismes différents (carte à puce avec mot de passe par exemple).

"Nom + mot de passe + date" sont cryptés avec des clés publiques et privées (RFC 1510). Le cryptage de la date évite la réutilisation éventuelle du message par un pirate. Par le cryptage on peut identifier de manière sûre l'utilisateur connecté. Pour éviter l'espionnage, la modification du contenu, l'ajout de message... on pourra utiliser la signature électronique (CRC crypté en fin de message) ou crypter toute l'information.

Les infrastructures PKI *(Public Key Infrastructure)* devraient se développer. Pour l'instant, le protocole SSL *(Secure Socket Layer)* domine toujours largement le marché de l'authentification sur les sites marchands. Radius, Tacacs ou IPSec (qui comporte un processus d'authentification dans son en-tête) constituent encore la solution retenue par la majorité des entreprises.

3.5.1 Cryptage symétrique

Une même clé est utilisée pour crypter et décrypter le message, très efficace et assez économe en ressources CPU cette technique pose le problème de la distribution des clés dans un réseau étendu (exemple DES, triple DES ou le récent AES).

3.5.2 Cryptage asymétrique

Chaque utilisateur dispose d'un jeu unique de clés, dont l'une est privée (secrète) et l'autre publique (exemple RSA). Pour recevoir des documents protégés, le détenteur d'un jeu de clés envoie sa clé publique à ses interlocuteurs, qui l'utilisent pour chiffrer les données avant de les lui envoyer. Seul le destinataire et détenteur des clés peut lire les informations en associant sa clé privée à sa clé publique. Cette technique nécessite des clés plus longues pour une sécurité équivalente.

3.5.3 Protocoles courants

SSL *(Secure Socket Layer)* de Netscape est le protocole le plus répandu pour établir une connexion sécurisée entre client et serveur. Il est situé entre les couches TCP et HTTP. Ce protocole public utilise une clé de 40 bits (version d'exportation) avec l'algorithme RSA pour chiffrer toute la transaction. Ce protocole ne peut garantir l'identité de l'interlocuteur !

SET *(Secure Electronic Transaction)* : est la convergence des deux procédures de sécurisation STT *(Secure Transaction Technology)* de Visa et Microsoft et SEPP *(Secure Electronic Payment Protocol)* de Mastercard, IBM et Netscape. Il permet de sécuriser les transactions par cartes bancaires (chiffrement par clés publiques/privées et authentification des parties).

C-SET *(Chip Secure Electronic Transaction)* : est l'adaptation du protocole SET à la carte à puce française.

S/MIME *(Secure Multipurpose Internet Mail Extension)* est le protocole le mieux accepté pour la sécurisation des courriers électroniques.

PGP *(Pretty Good Privacy)* **:**. Le cryptage de toute l'information par une clé publique nécessitant un temps de calcul élevé, PGP (***www.pgpi.com***) utilise une technique plus rapide : Le document est compressé (pour éviter les redondances) puis crypté avec une clé de session aléatoire (cryptage rapide), seule la clé de session est cryptée par la clé publique du destinataire et ajoutée au document. Le destinataire utilise sa clé privée pour décrypter la clé de session et peut ainsi décrypter le document et le décompresser.

3.5.4 PKI (Public Key Infrastructure)

L'infrastructure PKI repose sur la notion de chiffrement asymétrique. Pour s'authentifier, en revanche, le détenteur des clés utilise un certificat, sorte de document électronique faisant office de carte d'identité électronique. Inséré dans un message, lors d'un paiement sur Internet par exemple, ce certificat joue le rôle de signature numérique. Il contient des informations relatives à l'identité du détenteur, son champ d'application (date de validité, types d'applications, etc.) et la clé publique. Un tiers de confiance garantit l'association ente un individu et les données contenues dans le certificat.

La gestion des certificats en interne implique des infrastructures lourdes afin d'enregistrer les demandes, de vérifier la validité des certificats, de gérer les pertes ou les vols (risques d'autant plus importants lorsque le certificat est inclus dans un support physique tel qu'une carte à puce). Il faudra, de plus, assurer la protection des serveurs contre le piratage.

Difficile en interne, la gestion des infrastructures PKI peut être confiée à des prestataires spécialisés, tels que Certplus (en France) et Verisign (aux États-Unis), ou encore auprès d'une banque. Typiquement, un Français, client d'une banque française jouant le rôle de tiers certificateur, qui achète sur un site américain, aura du mal à imposer son certificat si son organisme bancaire n'est pas reconnu aux États-Unis comme un prestataire digne de confiance.

3.6 MESSAGERIES

Les messageries sont très utilisées et posent quelques problèmes de sécurité particuliers. De plus la majorité des virus utilisent actuellement ce vecteur.

3.6.1 Attaques

Spamming et mailbombing sont deux techniques, réprouvées par la Nétiquette, qui prennent pour cible votre boîte aux lettres, et peuvent vous faire perdre du temps, voire des données.

Sont notamment considérés comme étant des actes de spamming :

- le fait d'écrire à un inconnu pour lui demander par exemple de venir visiter votre site web;
- le fait d'inclure un individu dans une liste de diffusion sans son consentement;
- le fait de diffuser des messages sur un forum de discussion qui soient sans rapport avec le thème ou le contenu de ce dernier.

Le mailbombing est une variante belliqueuse du spamming qui consiste à encombrer volontairement la boîte aux lettres d'un destinataire par l'envoi de centaines de courriers électroniques vides, insultants ou volumineux, potentiellement accompagnés de virus en pièce jointe.

En épluchant l'en-tête des messages on tentera de retrouver l'adresse de l'émetteur ou au moins du premier serveur l'ayant relayé puis en écrivant à **postmaster@trucccc.com** ou **abuse@truccc.com** (d'après le nom du serveur SMTP utilisé par le spammer). Les administrateurs de relais peuvent filtrer certaines adresses en cas d'abus répétés. Bien que ce soit interdit par la RFC, certains message sont transmis avec les champs *to* et *cc* vides, votre adresse étant en *bcc* résultat, vous obtenez *to :Undisclosed.recipient@truc.com* remplis par le premier relais !

3.6.2 Sécurité des messages

- Confidentialité : seul le chiffrement peut l'assurer.
- Intégrité : le message reçu est identique à celui émis, le scellement et la signature électronique sont nécessaire.
- Contrôle d'accès : uniquement les personnes autorisées peuvent émettre des messages
- Non répudiation : utilisation d'un tiers de confiance.

3.6.3 Spamming

On appelle « spam » la diffusion en masse de messages, publicitaires généralement, non désirés par les destinataires. Originellement « spam » désigne du jambon en conserve de basse qualité *(Shoulder of Pork and hAM).*

Il est souvent inutile de répondre rageusement à l'émetteur car il a souvent disparu. Pour éventuellement retrouver le FAI émetteur on épluchera l'entête du message ou on consultera ***spamcop.net*** . L'adresse ***abuse@nom_du_fai.com*** doit exister et pourra servir à alerter le FAI. Les adresse utilisées dans les forums sont souvent exploitées pour du spam, il pourra être judicieux d'utiliser alors une adresse provisoire (chez ***www.spammotel.com*** par exemple).

ATTENTION : Un serveur SMTP ne devrait jamais être laissé en « open relay » car il est alors ouvert et cette configuration est facilement détectable. Les « spammer » pourront alors l'utiliser à votre insu et vous risquez d'être boycotté par les autres sites !

- Collectif anti spam ***www.cspam.org***
- Les serveurs envoyant du « spam » sont répertoriés par ***www.mail-abuse.org*** .
- DSBL *(Distributed Sender Boycott List)* liste des serveurs SMTP ouverts ***www.dsbl.org***
- ***www.mailwasher.net*** édite un logiciel qui bloque les spam avant téléchargement et envoie automatiquement un message d'erreur à l'expéditeur.

3.7 DÉTECTION D'INTRUSION

Même si l'intrus parvient à franchir les barrières de protection (coupe-feu, système d'authentification, etc.), il est encore possible de l'arrêter avant qu'il n'attaque. Placés sur le réseau de l'entreprise, les outils de détection d'intrusion décèlent tout comportement anormal ou trafic suspect.

Malgré la mise en place de solutions d'authentification, chargées de filtrer et de contrôler les accès au réseau, il arrive que des intrus y pénètrent. C'est même le propre des pirates que de contourner les serveurs d'authentification, coupe-feu et autres barrières de protection des systèmes. Une fois entrés, plus rien ne les empêche de saboter, de voler et d'endommager les applications. Interviennent alors les systèmes de détection d'intrusion. En auscultant en permanence le trafic, ils repèrent le *hacker* et alertent aussitôt l'administrateur. Protégeant

l'entreprise des attaques externes, ces systèmes sont également capables de détecter le pirate interne qui représente encore entre 70 à 80% des actes de malveillance auxquels sont confrontées les sociétés. Il existe deux catégories d'outils sur le marché : la première analyse le trafic réseau, la seconde étudie le comportement des utilisateurs au niveau d'un système ou d'une application.

Dans tous les cas, des ressources humaines devront être affectées à la supervision des systèmes de détection d'intrusion pour gérer les alertes, mais aussi pour détecter ce que les outils n'auront peut-être pas vu. Coûteuses, ces ressources freineraient aujourd'hui les entreprises dans l'adoption de ces solutions.

3.7.1 Surveillance du trafic réseau

Baptisés sondes ou encore *sniffer,* ce sont des outils de détection d'intrusion qui s'installent à un point stratégique du réseau. Ils analysent en permanence le trafic à la recherche d'une signature connue de piratage dans les trames. Ces systèmes ne repèrent que les attaques qui figurent déjà dans leur base de signatures. Ces sondes doivent être :

- Puissantes (débits des réseaux élevés) pour analyser toutes les trames.
- Capables de conserver un historique (actes de malveillance divisés sur plusieurs trames).
- Fiable, c'est à dire tolérante aux pannes (retour à l'état initial après une interruption).

3.7.2 Analyse du comportement de l'utilisateur

Installée sur les OS ou sur les applications, l'analyse du comportement scrute les fichiers d'événements et non plus le trafic. Cette technique est encore trop coûteuse car trop de compétences sont nécessaires.

Des agents sont placés sur le système ou l'application supervisés. Ces agents autonomes disposent de capacité d'apprentissage. Leur mission consiste à repérer tout abus (personne qui cherche à outrepasser ses droits et à atteindre des applications auxquelles elle n'a pas accès) ou comportement suspect (personne qui, par exemple, scanne toute une base de données alors qu'en temps normal, elle n'effectue que deux à trois requêtes par jour). De même, le transfert de certains courriers peut être bloqué lorsque ces documents comportent certains mots (préalablement déterminés par l'administrateur) pouvant indiquer la fuite d'informations. Pour être efficaces, ces solutions doivent bénéficier d'une puissance suffisante afin d'analyser tous les événements en temps réel, mais aussi de mécanismes qui les protègent des attaques.

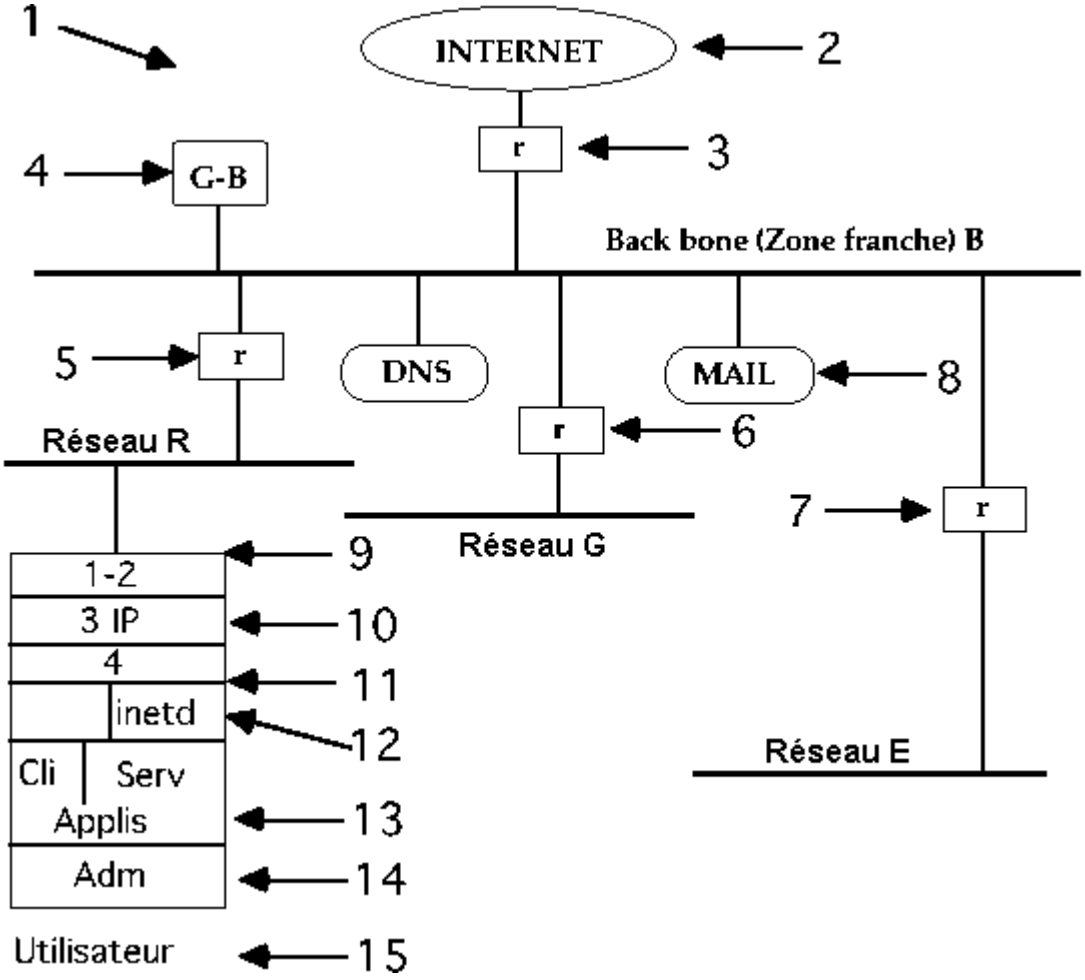
3.7.3 Site « pot de miel »

Ces sites « honey pot » sont sensés détourner les pirates des zones sensibles en leur donnant l'impression qu'ils sont entrés au cœur du site de l'entreprise visée.

L'efficacité reste à démontrer, il semblerait que ce soit suffisant pour se protéger des amateurs (les plus nombreux !).

3.8 OÙ AGIR

Exemple sur un réseau avec routeurs Unix (source J-L Archimbaud / UREC)



1. architecture physique et logique du réseau
2. réseau G "inconnu"
3. annoncer uniquement R et B
4. Garde-barrière
5. filtrer le réseau E
6. ne router que R et B, filtrer / applications et stations
7. ne router que R et B
8. installer un "bon" sendmail
9. pas de ifconfig
10. pas de "route default"
11. filtres et trace ---> tcpd, xinetd
12. inetd.conf
13. applications sécurisées : PGP
14. surveiller - contrôler : COPS, CRACK
15. sensibiliser, charte

Une protection efficace utilisera un « Firewall », un antivirus, un IDS, un VAT, une politique d'administration, des locaux protégés, une formation des utilisateurs à la confidentialité…

3.9 TESTS

3.9.1 Tests de maintenance

- **PING** : permet de vérifier l'accessibilité à une machine spécifiée. Si le ping est correct et pas l'accès Web, il y a probablement un problème de port ou de répertoire non valide. (***www.fr.net/internet/ping.html***).
- **TRACEROUTE** : permet de déterminer le chemin d'un point à un autre avec les délais (envoi de 3 paquets ICMP peu prioritaires donc les temps ne sont pas toujours très significatifs). Windows95 propose l'utilitaire DOS "TRACERT" et ***www.fr.net/trace.html*** donne l'adresse de sites offrant ce test.
- **FINGER** : permet de connaître les caractéristiques d'un utilisateur connecté (normalement ce service est filtré !).
- ***www.samspade.org*** propose un outil (libre) pour retrouver l'adresse d'un expéditeur (anonyme ?) et divers outils.
- **HPING, Nemesis, SPAK** : ces outils permettent d'émettre des requêtes TCP simples ou de créer ses propres paquets IP (test de ports…) ***www.hping.org***
- **SNMP :** Attention, si ce service est monté en «community string =public», toutes les informations sur le réseau sont disponibles !
- **SMTP :** la commande « vrfy » permet de recenser les utilisateurs avec leur adresse et « expn » permet de vérifier les alias et listes.

3.9.2 Logiciels de test de la sécurité d'une installation

Au delà de 200 machines une automatisation des tests est nécessaire. On pourra utiliser des logiciels de détection de vulnérabilité (VAT : *Vulnerability Assessment Tools*). Ils ont le même point faible que les antivirus : leur base de signatures. Celle-ci doit être mise à jour régulièrement, sans quoi le rapport de vulnérabilité risque fort d'être erroné..

La détection des vulnérabilités s'effectue via des scénarios. Ces derniers, proposés par les éditeurs, sont modifiables afin de coller aux spécificités de l'entreprise.

Les systèmes de détection d'intrusions peuvent être classés selon leur position :

- NIDS : *Network Intrusion Detection System*, cousins des analyseurs réseaux (Snort, Netsecure…), inefficace sur VPN ou VLAN (cryptage) voire sur Gigabit.
- HIDS : *Host based IDS*, similaire aux outils d'administration de service, vérifie l'usage d'une ressource ou d'un service par un utilisateur (Intruder alert, dragon squire…).
- NNIDS : *Network Node IDS*, complémentaire d'un OS, effectue un IDS sur la machine hôte et évite ainsi les problèmes de cryptage ou de rapidité du réseau (Black Ice, Tiny CMDS…).

Quelques logiciels courants :

- **SATAN** : freeware permettant le test de machines UNIX sur un réseau ***(ftp://ftp.cert.dfn.de/pub/tools/net/satan)*** produit périmé.
- **COPS** *(Computer Oracle and Password System)* : test de la machine Unix sur lequel le logiciel est installé. ***(ftp://ftp.cert.org/pub/tools/cops).***
- **Crack** : freeware testant les mots de passe Unix (etc/password).
- **Lophtcrack** (NT) cracker et sniffeur de mot de passe.
- **John the ripper** (free, Win/Unix) crack de mot de passe.

- **ISS** *(Internet Security System)* : Logiciel public, historiquement, ISS, avec son outil Internet Scanner, disposait de la base de signatures la plus riche. Depuis, il ne cesse de perdre du terrain. La solution d'ISS se compose de trois modules : Internet Scanner (logiciel testé), System Scanner et Database Scanner, ils détectent respectivement les vulnérabilités réseaux, systèmes et applicatives (bases de données) ***www.iss.net*** .
- **Nessus** freeware récent de test d'intrusion (***www.nessus.org***).
- **NetRecon** *(Axent Technology)* : scanner classique (installé sur un poste).
- **Security Analyzer** *(Web trend)* : WebTrends a opté pour une technologie de type agents/manager/console. Les agents ne sont pas indispensables au fonctionnement du produit, mais vivement recommandés si l'on souhaite obtenir une évaluation exhaustive. Ces agents sont déployés sur les équipements à surveiller
- **CyberCop Scanner** *(Network Associates)* : Network Associates s'enorgueillit de proposer une base de signatures référençant plus de 730 vulnérabilités avérées
- **Snort** : logiciel de détection d'intrusion ***www.snort.org***

3.9.3 Certification des produits de sécurité

A l'origine, seule la certification européenne « itsec » (dérivée du « orange book » du DOD américain) avec ses 6 niveaux E1..E6 est disponible (cartes à puces…).

La norme ISO 15408 définit les fonctionnalités et garanties sécuritaires d'un produit. Il y a 7 niveaux d'évaluation EAL1 (tests fonctionnels) à EAL7 (produits stratégiques avec vérification de chaque détail). Les certificats sont délivrés sous couvert de la DCSSI *(Direction Centrale de la Sécurité des Systèmes d'Information)* via des laboratoires agréés appelés CESTI *(Centre de certification de la sécurité des technologies de l'information)*.

La norme ISO 17799, issue de la norme Anglaise BS7799, est dédiée à la mise en œuvre d'une sécurité des systèmes d'information et permet de certifier une entreprise. Elle est compatible ISO 9001.

4 DOCUMENTATIONS

4.1 Informations sur la sécurité

- CRU *(comité réseau des universités)* à ***www.cru.fr***
- UREC-CNRS ***www.urec.cnrs.fr/securite***
- CNIL *(commission nationale de l'informatique et des libertés)* permet de vérifier les informations qu'un site peut obtenir sur vous lors de votre navigation (adresse, nom…) ***www.cnil.fr*** .
- Secuser (fr) : infos sur les virus et autres… ***www.secuser.com***
- Sécurité des systèmes : ***www.secusys.com***
- Portail sécurité (fr), logiciels libres : ***www.securite.org***
- CLUSIF *(Club de la sécurité des systèmes d'information Français) à* ***www.clusif.asso.fr*** .
- DCSSI *(Direction Centrale de la Sécurité des Systèmes d'Information)* ***www.scssi.gouv.fr*** .
- AURIF *(association des utilisateurs de réseaux île de France)* ***www.aurif.fr***
- OSSIR *(Observatoire de la sécurité des systèmes d'information et des réseaux)* ***www.ossir.org***
- SUR *(sécurité Unix et réseaux)* ***www.ossir.org/sur***
- Web securité ***http://websec.arcady.fr***
- Veille et conseil : ***www.cartel-securite.fr***
- Consultant en sécurité : ***www.hsc.fr***
- MISCMAG (revue dédiée à la sécurité) ***www.miscmag.com***
- CERT *(Computer Emergency Response Team)* organisme officiel américain publiant des alertes de sécurité. ***www.cert.org***, ***www.eurocert.net***
- Bugtraq : mailing list des problèmes de sécurité.
- Collectif anti spam ***www.cspam.org***
- DSBL *(Distributed Sender Boycott List)* liste des serveurs SMTP ouverts ***www.dsbl.org***
- EICAR *(European Institute for Computer Antivirus Research)* ***www.eicar.com***
- NT bug traq *(sécurité sur Windows NT)* ***www.ntbugtraq.com*** **.**
- NCSA *(National Computer Security Association)* à ***www.ncsa.com***
- SANS *(System Administration, Networking & Security)* à ***www.sans.org***
- Security focus ***www.securityfocus.com***
- NITC *(National Infrastructure Protection Center)* ***www.nitc.gov***
- NIST *(National Institute of Standards and Technology)* pour le cryptage AES ***http://csrc.nist.gov/encryption/aes***
- ISS *(Internet Security System)* ***www.iss.net***
- CIS ***www.cisecurity.org*** outils d'audit gratuits.
- PGP *(cryptage)* ***www.pgp.com*** ***ou*** ***www.pgpi.com***
- Infos « Underground » ***www.zataz.com*** , ***www.phrack.com***
- ***www.attrition.org*** répertorie les attaques et bugs.
- les "crackers" publient dans ***www.2600.com*** ou sur les news (alt.2600).
- RFC 2196 *Site Security Handbook* : sécurité des informations et des installations.
- RFC 2504 *Users' Security Handbook* : sécurité utilisateur.

4.2 Acronymes

AES : Advanced Encryption Standard (cryptage).
DES : Data Encryption Standard (cryptage).
IDS : Intrusion Detection System.
MSSP : Managed Security Service Providers (fournisseurs de services de sécurité).
PGP : Pretty Good Privacy (Protocole de cryptographie à double clé).
PKI : Public Key Infrastructure (chiffrement).
RADIUS : Remote Access Dial In User Server (authentification d'un abonné).
RAID : Redundancy Array of Inexpensive/Independent Disk (archivage).
RSA : Rivest Shamir and Adleman (algorithme de cryptage).
SPAM : *« Shoulder of Pork and hAM » (jambon en conserve*), email publicitaire.
SANS : System Administration, Networking & Security.
SSL : Secure Socket Layer (protocole de sécurité sur HTML).
TACACS : Terminal Access Controller Access Control System (authentification).
VAT : Vulnerability Assessment Tools (outils de vérification de vulnérabilité).
VPN : Virtual Private Network. (tunnel sur réseaux publics).