ISTA Mohamed EL FASSI - Errachidia

Filière : Techniques de Réseaux Informatiques

Support de formation

Module :

NOTIONS DE SÉCURITÉ DES RÉSEAUX INFORMATIQUES

Elaboré par : A. EL GHATTAS

Septembre 2008

http://adnaneadnane.ifrance.com/

Super.Adnane@hotmail.fr

I. Introduction à la sécurité et les risques menaçant les sites informatiques

1. Introduction

Au fil des dernières décennies, les outils informatiques ont acquis une grande importance dans tous les domaines de la vie professionnelle et privée, du fait qu'ils permettent d'accomplir un nombre croissant de tâches de toute nature et du fait qu'ils deviennent de plus en plus maniables et aisés à utiliser.

Cependant, l'importance acquise par les systèmes informatiques dans le traitement de données les transforme également en cibles préférées pour des attaques et des tentatives d'intrusion sur différents niveaux. Ce risque est d'autant plus accru par l'ouverture progressive des systèmes à l'extérieur par la connexion à Internet.

S'y ajoutent les risques « classiques » tels que le manque de vigilance de la part de certains usagers ou des sinistres comme le feu, l'inondation et la coupure de courant.

Les systèmes évoluent dans des conditions changées, exigeant une sécurisation plus fondamentale et plus efficace. Cette sécurisation ne doit pas se limiter uniquement à l'aspect purement technique, mais elle doit impliquer tous les acteurs concernés (responsables du traitement, employés exécutants et sous-traitants, personne dont des données sont traitées). Il s'agit donc de combiner des mesures techniques et logiques à des mesures organisationnelles, impliquant une organisation bien structurée, la sensibilisation et la vigilance de tous les acteurs.

2. Objectifs de la sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs :

La confidentialité

La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

L'intégrité

Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

La disponibilité

L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources.

La non-répudiation

La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

L'authentification

L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

3. Classification des risques

Le risque en terme de sécurité est généralement caractérisé par l'équation suivante :

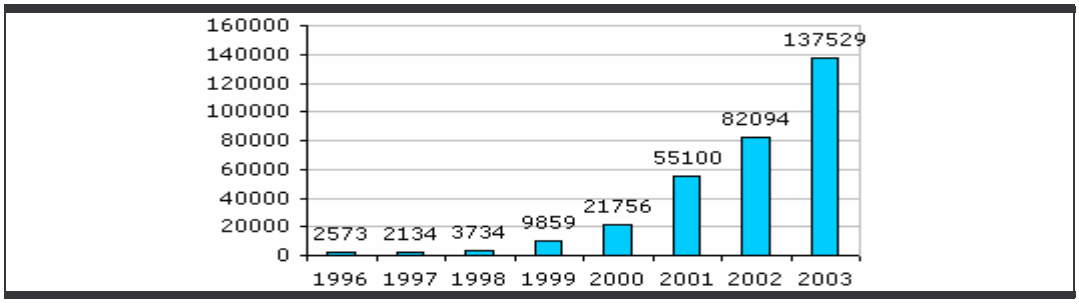
$$\text{risque} = \frac{\text{menace} \times \text{vulnérabilité}}{\text{contre-mesure}}$$

La **menace** représente le type d'action susceptible de nuire dans l'absolu, tandis que la **vulnérabilité** représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin la **contre-mesure** est l'ensemble des actions mises en oeuvre en prévention de la menace.

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

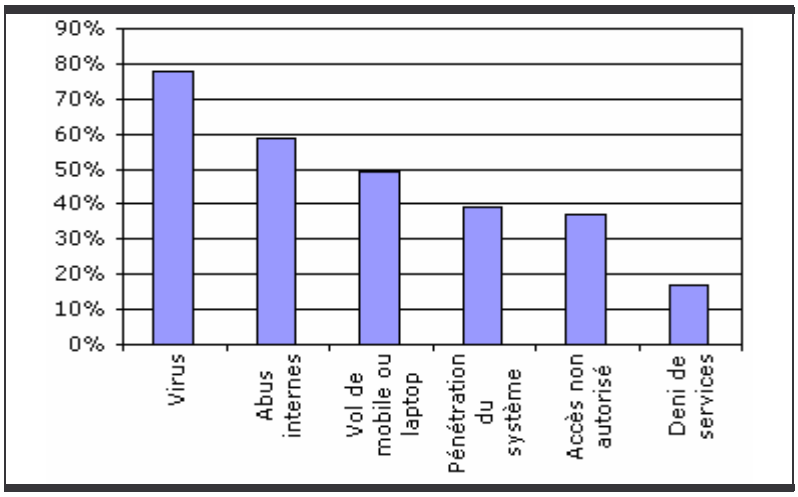
Les principales menaces effectives auxquelles on peut être confronté sont :

- **l'utilisateur** : l'énorme majorité des problèmes liés à la sécurité d'un système d'information est l'utilisateur (par insouciance ou malveillance)
- les **programmes malveillants** : un logiciel destiné à nuire ou à abuser des ressources du système est installé (par mégarde ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données
- **l'intrusion** : une personne parvient à accéder à des données ou à des programmes auxquels elle n'est pas censée avoir accès
- un **sinistre** (vol, incendie, …) : une mauvaise manipulation ou une malveillance entraînant une perte de matériel et/ou de données.



Nombre d'incidents connus liés à la sécurité informatique répertoriés par le CERT

(source : http://www.cert.org/)



CSI/FBI 2004 Computer Crime and Security Survey Results

(source : http://www.gocsi.com)

4. Exemples de menaces

a. Risque naturels

Plusieurs risques peuvent menacer la sécurité d'un système informatique : inondation, tremblement de terre, foudre… mais le principal risque reste les incendies surtout celles d'origine électrique.

En effet, un incendie sur trois est d'origine électrique. Les principales causes de ces incendies sont :

- L'échauffement par surintensité : dégagement de chaleur lié à la résistance du récepteur et à l'intensité ;
- La surintensité par surcharge : une intensité supérieure à ce que peut supporter un circuit ;
- Le court-circuit ….

Certains facteurs peuvent aggraver les échauffements :

- Une ventilation insuffisante ;
- L'accumulation de poussière ou de dépôts de graisse ;
- Le stockage de matériaux inflammables à proximité d'installations électriques ;
- …

b. Les virus

Nous dirons ici que tout Code Parasite Autopropageable (CPA) est un virus informatique (définition de Mark Ludwig, tirée de The Little Book of Computers Viruses, 1991). Le terme «code» fait bien évidemment référence à des instructions rédigées dans un langage de programmation évolué ou non. Le mot « parasite » souligne le caractère insidieux du code viral : il est là où on ne devrait normalement pas le trouver. Il constitue un ajout non-voulu par l'utilisateur. Quant à « autopropageable », il renvoie à cette caractéristique de duplication qu'ont les virus : la capacité à se multiplier en infectant d'autres fichiers. Ils recopient leurs propres instructions (code) au sein de celles d'un autre programme. L'efficacité de la duplication se mesure au fait que l'exécution du programme hôte n'est pas altérée, alors que ses fonctionnalités ont été modifiées. C'est une définition parmi tant d'autre d'un virus informatique mais intéressons nous maintenant aux différents types qui existent.

Notion d'antivirus

Un antivirus est un programme capable de détecter la présence de virus sur un ordinateur et, dans la mesure du possible, de désinfecter ce dernier. On parle ainsi d' « éradication » de virus pour désigner la procédure de nettoyage de l'ordinateur.
Il existe plusieurs méthodes d'éradication :

- La suppression du code correspondant au virus dans le fichier infecté ;
- La suppression du fichier infecté ;
- La mise en quarantaine du fichier infecté, consistant à le déplacer dans un emplacement où il ne pourra pas être exécuté.

La détection des virus

Les virus se reproduisent en infectant des "applications hôtes", c'est-à-dire en copiant une portion de code exécutable au sein d'un programme existant. Or, afin de ne pas avoir un fonctionnement chaotique, les virus sont programmés pour ne pas infecter plusieurs fois un même fichier. Ils intègrent ainsi dans l'application infectée une suite d'octets leur permettant de vérifier si le programme a préalablement été infecté : il s'agit de la **signature virale**.
Les antivirus s'appuient ainsi sur cette signature propre à chaque virus pour les détecter. Il s'agit de la méthode de **recherche de signature** (scanning), la plus ancienne méthode utilisée par les antivirus.
Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus. Toutefois cette méthode ne permet pas la détection des virus n'ayant pas encore été répertoriés par les éditeurs d'antivirus. De plus, les programmeurs de virus les ont désormais dotés de capacités de camouflage, de manière à rendre leur signature difficile à détecter, voire indétectable; il s'agit de "**virus polymorphes**".
Certains antivirus utilisent un **contrôleur d'intégrité** pour vérifier si les fichiers ont été modifiés. Ainsi le contrôleur d'intégrité construit une base de données contenant des informations sur les fichiers exécutables du système (date de modification, taille, et éventuellement une somme de contrôle). Ainsi, lorsqu'un fichier exécutable change de caractéristiques, l'antivirus prévient l'utilisateur de la machine.

Types de virus
On peut classer les virus selon leur mode de déclenchement ou leur mode de propagation. On distingue alors plusieurs catégories de virus :

• **Les vers** : il s'agit de programmes possédant la faculté de s'autoreproduire et de se déplacer à travers un réseau en utilisant les mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier ...) pour se propager. Un ver (en anglais worm) est donc un virus réseau. Ces virus se servent des programmes de messagerie (notamment Microsoft Outlook) pour se répandre à grande vitesse, en s'envoyant automatiquement à des personnes présents dans le carnet d'adresses. Leur premier effet est de saturer les serveurs de messagerie, mais ils peuvent également avoir des actions destructrices pour les ordinateurs contaminés. Ils sont particulièrement redoutables, car le fait de recevoir un mail d'une personne connue diminue la méfiance du destinataire, qui ouvre alors plus facilement le fichier joint contaminé.

• **Les bombes logiques** : elles sont de véritables bombes à retardement. Ce sont de petits programmes restant inactifs tant qu'une condition n'est pas remplie, une fois la condition remplie (une date par exemple), une suite de commandes est exécutée (dont le but, le plus souvent, hélas, est de faire le plus de dégâts possible).
Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise !

• **Les chevaux de Troie** : (en anglais trojan horse) par analogie avec la mythologie grecque, ce sont des programmes dont l'aspect malveillant est caché au premier abord. Un cheval de Troie permet généralement de préparer une attaque ultérieure de la machine infectée.
Par exemple, ils agissent en laissant ouverts des ports de communication qui peuvent être ensuite utilisés par des programmes d'attaque. Ils sont difficiles à détecter par un utilisateur non averti.
Un cheval de Troie est donc un programme caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à la machine sur laquelle il est exécuté. Un cheval de Troie peut par exemple :

- voler des mots de passe
- copier des données sensibles
- exécuter tout autre action nuisible
- ...

• **Les macrovirus** : ce sont des virus écrits sous forme de macros (une macro est une série de commandes destinée à effectuer automatiquement quelques tâches d'une application spécifique) exécutables dans des applications bureautiques (traitement de texte, tableur, etc.) ou des logiciels clients de messagerie électronique. Ces macrovirus vont détourner tous les appels des macros standards. La propagation se fait généralement par l'opération de sauvegarde. Comme de plus en plus de logiciels intègrent ces notions de macros, les macrovirus sont devenus les virus les plus fréquents et les plus redoutables pouvant malheureusement causer de grands dégâts (formatage du disque dur par exemple). Un tel virus peut être situé à l'intérieur d'un banal document Word ou Excel, et exécuter une portion de code à l'ouverture de celui-ci lui permettant d'une part de se propager dans les fichiers, mais aussi d'accéder au système d'exploitation (généralement Windows).

• **Les virus de secteur d'amorce** (aussi appelés virus « boot sector ») : cette catégorie regroupe les virus infectant le secteur d'amorçage du disque (disque dur, disquettes...). Il s'agit d'un type de virus infectant la partie faisant démarrer l'ordinateur.
Ce type de virus est de nos jours peu contagieux. Pour qu'un ordinateur soit infecté, il doit être démarré avec un secteur d'amorçage infecté, ce qui était courant sur les premiers ordinateurs mais qui est rare aujourd'hui. Pourtant ce genre de virus est fort dangereux. En effet, il se trouve dans le premier secteur du disque et est donc chargé à chaque allumage de l'ordinateur. Le secteur d'amorçage du disque est le premier secteur lu au démarrage de l'ordinateur.

• **Les virus fichiers :**
Virus Non résidents : C'étaient les virus les plus répandus il y a quelques années. Lors de l'infection, il cherche un fichier cible, et remplace, par sa section virale, le premier segment du programme. La section originale est alors ajoutée en fin de programme. Au moment de l'exécution du fichier, c'est le code viral qui est d'abord lancé. Ce code viral cherche d'autres programmes à infecter, il les infecte. Ensuite il restitue la première section du programme infecté et l'exécute celui-ci. La boucle est bouclée. Le virus a pu se propager de façon tout à fait invisible. Il s'agit donc d'un virus fort contagieux. La détection de ce genre de virus est pourtant assez aisée, le fichier infecté étant plus grand que le fichier sain, puisqu'il contient le virus en plus du programme.

Virus résidents : Il s'agit de virus qui restent présent dans la mémoire de l'ordinateur (RAM, à ne pas confondre avec le disque dur qui peut aussi être appelé mémoire). Fonctionnement : Une fois un fichier infecté exécuté (NB : ce fichier infecté vient soit d'une source infectée, une source douteuse, soit d'un autre fichier infecté précédemment), le virus se loge dans la mémoire vive, ou il reste actif. Dès qu'un programme est exécuté et qu'il n'est pas infecté, le virus l'infecte.
La différence avec celui vu précédemment est qu'il n'y a pas besoin de procédure pour trouver une cible, puisque c'est l'utilisateur qui la désigne en exécutant le programme cible. Ce genre de virus est actif à partir du moment où un programme infecté est exécuté jusqu'à l'arrêt complet de la machine.

Virus multiformes : Virus regroupant les caractéristiques des virus parasites et des virus du secteur d'amorçage.

Les autres caractéristiques des virus sont :
Virus furtifs (intercepteurs d'interruptions) : ce sont des virus modifiant complètement le fonctionnement du système d'exploitation. Ces virus le modifient tellement qu'il semble sain aux antivirus. Ceci les rend très difficiles à détecter, puisque les antivirus sont trompés, croyant le système d'exploitation sain.

Virus polymorphes (mutants) : ce virus est différent à chaque infection. Il doit ceci à son encryption (Il existe un algorithme reprenant une valeur au hasard, permettant d'avoir un fichier crypté à chaque fois différent ne dérangeant cependant pas le décryptage). Le programme entier et le virus sont encryptés, excepté le premier segment destiné à la décryption. Ce genre de virus est donc beaucoup plus difficile à détecter que les précédents et presque impossible à détruire sans supprimer le fichier infecté, vu qu'il est crypté.

Virus flibustiers (Bounty hunters) : virus visant la modification des antivirus les rendant non - opérationnels. Ce genre de virus est très rare mais très efficace.

Il faut savoir que un virus peut regrouper une, plusieurs, voire toutes les caractéristiques vues ci-dessus. Plus le virus a de caractéristiques, plus il sera dangereux, compliqué, vorace en ressources de l'ordinateur (dû à sa complexité). Ce qui signifie gênant sans même être actif, et surtout difficile à détecter par un antivirus (trompé, rendu inactif, ...) mais aussi plus facilement repérable, et ce, dû à la baisse des performances de la machine.

• **Les virus VBS script** : Ce type de virus se propage par mail à l'aide d'un fichier attaché (type exe, vbs etc..) bien souvent en ayant un nom évocateur. Ces nombreux virus sont en langage Visual Basic. Ils sont de type Vbs (Visual Basic Script) ou plus simplement «script ». Par exemple, le désormais célèbre « I Love You » est écrit dans ce langage.

• **Les canulars** : Depuis quelques années un autre phénomène est apparu, il s'agit des canulars (en anglais **hoax**), c'est-à-dire des annonces reçues par mail propageant de fausses informations (par exemple l'annonce de l'apparition d'un nouveau virus destructeur ou bien la possibilité de gagner un téléphone portable gratuitement,...) accompagnées d'une note précisant de faire suivre la nouvelle à tous ses proches. Ce procédé a pour but l'engorgement des réseaux ainsi que la désinformation.
Ainsi, de plus en plus de personnes font suivre des informations reçues par courriel sans vérifier la véracité des propos qui y sont contenus. Le but des hoax est simple : provoquer la satisfaction de son concepteur d'avoir berné un grand nombre de personnes.

c. Spam
Le spam, mot anglais du jargon informatique, désigne les communications électroniques massives, notamment de courrier électronique, sans sollicitation des destinataires, à des fins publicitaires ou malhonnêtes.
En guise de remplacement, certains pays francophones proposent d'utiliser les mots **pourriel** (de poubelle et courriel) et **polluriel** (de pollution et courriel), ainsi que d'autres variantes. Le mot pourriel est d'usage assez courant.
Le verbe **spammer** est souvent utilisé dans le langage familier pour qualifier l'action d'envoyer du spam, le spamming. Le mot spammeur désigne celui qui envoie du spam.

Cibles du pourriel :
Le pourriel peut s'attaquer à divers médias électroniques : les courriels, les forums de discussion, les moteurs de recherche, ….

- **Par courrier électronique :**

Le pourriel par courrier électronique est le type de pollupostage le plus répandu. Le coût d'envoi d'un courrier électronique étant négligeable, il est facile d'envoyer un message à des millions de destinataires. Les destinataires assument le coût de réception et de stockage en boîte aux lettres, ce qui peut causer des coûts non négligeables aux prestataires de services, à cause du volume pris par le pourriel.
Les forums de discussion sont une cible facile du spam. En effet, un message envoyé à un forum touche tous les lecteurs du forum. Certains groupes de discussion ne reçoivent pratiquement plus que du pollupostage (c'est l'une des raisons pour lesquelles de nombreux forums sont modérés, c'est-à-dire surveillés par un humain ou un robot qui effectue un tri parmi les articles proposés).

- **Par des fenêtres pop-up de Windows.**
- **….**

d. Spyware

Spyware ou logiciel espion (se dit également espiogiciel) est un logiciel malveillant qui infecte un ordinateur dans le but de collecter et de transmettre à des tiers des informations de l'environnement sur lequel il est installé sans que l'utilisateur n'en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet, qui sert de moyen de transmission des données.

- **Fonctionnement**

Un logiciel espion est composé de trois mécanismes distincts :

- Le mécanisme d'infection. Par exemple, le spyware Cydoor utilise le logiciel grand public Kazaa.
- Le mécanisme assurant la collecte d'information. Pour le même exemple, la collecte consiste à enregistrer tout ce que l'utilisateur recherche et télécharge via le logiciel Kazaa.
- Le mécanisme assurant la transmission à un tiers. Ce mécanisme est généralement assuré via le réseau Internet. Le tiers peut être le concepteur du programme ou une entreprise.

- **Où trouve-t-on des logiciels espions ?**

Le logiciel espion est très répandu sur les systèmes Microsoft, sur lesquels il n'est généralement pas détectable par les logiciels antivirus ni les anti-espiogiciels actuels. Certaines pages web peuvent, lorsqu'elles sont chargées, installer à l'insu de l'utilisateur un logiciel espion, généralement en utilisant des failles de sécurité du navigateur Internet Explorer.

Ils sont souvent présents dans des gratuiciels afin de rentabiliser leur développement. Il est possible que la suppression de l'espiogiciel d'un gratuiciel empêche celui-ci de fonctionner. En général les logiciels à code source libre comme Mozilla FireFox n'en contiennent aucun.

On en trouve également dans les logiciels d'installation de pilotes fournis avec certains périphériques. Ainsi, les fabricants d'imprimantes peuvent s'en servir pour savoir en combien de temps une cartouche d'encre est vidée. Plus généralement, tous les logiciels propriétaires peuvent en cacher puisque leurs sources ne sont pas accessibles.

Enfin, certains administrateurs systèmes ou réseaux installent eux-mêmes ce type de logiciel pour surveiller à distance l'activité de leurs ordinateurs, sans avoir à se connecter dessus.

II. Attaques informatiques

1. Introduction

Tout ordinateur connecté à un réseau informatique peut potentiellement vulnérable à une attaque.

Sur Internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont en réalité généralement lancées automatiquement à partir de machines infectées (virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire et plus rarement par des pirates informatiques.

On appelle «attaque réseau» l'exploitation d'une faille (du système d'exploitation, d'un logiciel communiquant par le réseau ou bien même de l'utilisateur) à des fins non connues par la victime et généralement préjudiciables.

Le but peut être de différentes sortes :

- obtenir un accès au système
- obtenir des informations personnelles sur l'utilisateur
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.)
- faire dysfonctionner un service….

2. Typologies de pirates

Qu'est-ce qu'un hacker ?

Le terme «hacker» est souvent utilisé pour désigner un pirate informatique. Ce terme a eu plus d'une signification depuis son apparition à la fin des années 50. A l'origine ce nom désignait d'une façon méliorative les programmeurs émérites, puis il servit au cours des années 70 à décrire les révolutionnaires de l'informatique, qui pour la plupart sont devenus les fondateurs des plus grandes entreprises informatiques.
C'est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
Aujourd'hui ce mot est souvent utilisé à tort pour désigner les personnes s'introduisant dans les systèmes informatiques

Les différents types de pirates

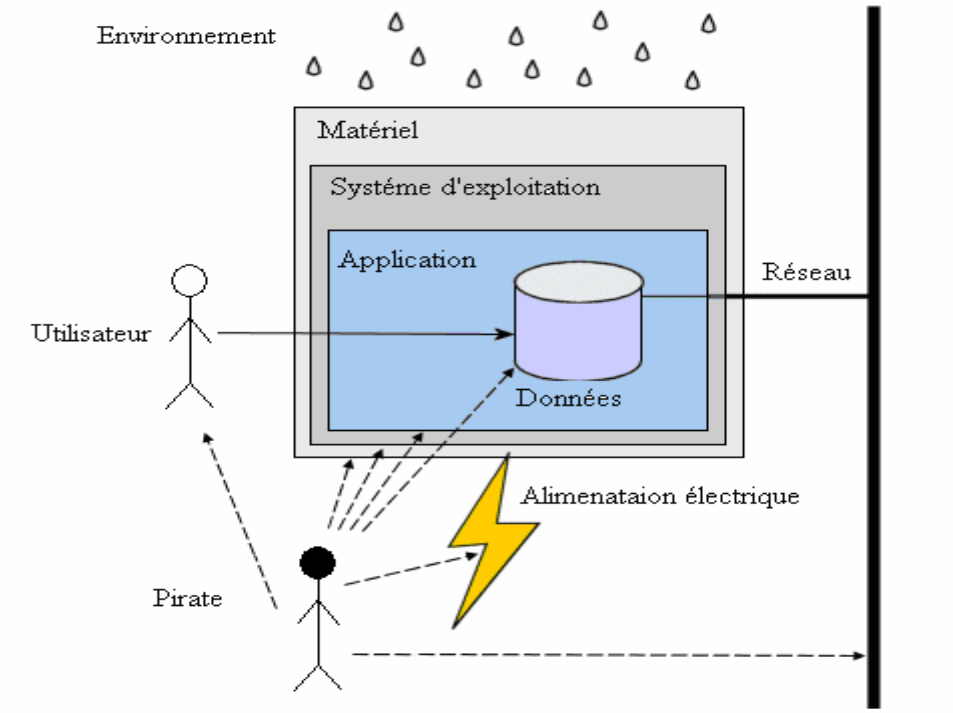
En réalité il existe de nombreux types d'"attaquants" catégorisés selon leur expérience et selon leurs motivations :

- Les white hat hackers, hacker au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques, sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui. Le courrier électronique en est un exemple
- Les black hat hackers, plus couramment appelés pirates (ou appelés également crackers par extension du terme), c'est-à-dire des personnes s'introduisant dans les systèmes informatiques dans un but nuisible
    - Les Script Kiddies (traduisez gamins du script, parfois également surnommés crashers, lamers ou encore packet monkeys, soit les singes des paquets réseau) sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques afin de s'amuser.
    - Les phreakers sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de téléphoner gratuitement grâce à des circuits électroniques connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement.
    - Les carders s'attaquent principalement aux systèmes de cartes à puces (en particulier les cartes bancaires) pour en comprendre le fonctionnement et en exploiter les failles.
    - Les crackers sont des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants. Un «crack» est ainsi un programme créé exécutable chargé de modifier (patcher) le logiciel original afin d'en supprimer les protections.
- Les hacktivistes (contraction de hackers et activistes que l'on peut traduire en cybermilitant ou cyberrésistant), sont des hackers dont la motivation est principalement idéologique. Ce terme a été largement porté par la presse, aimant à véhiculer l'idée d'une communauté parallèle (qualifiée généralement de underground, par analogie aux populations souterraines des films de science-fiction).

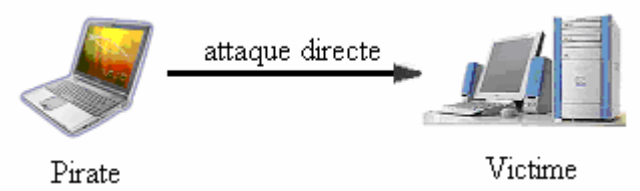
3. Types d'attaques

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

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



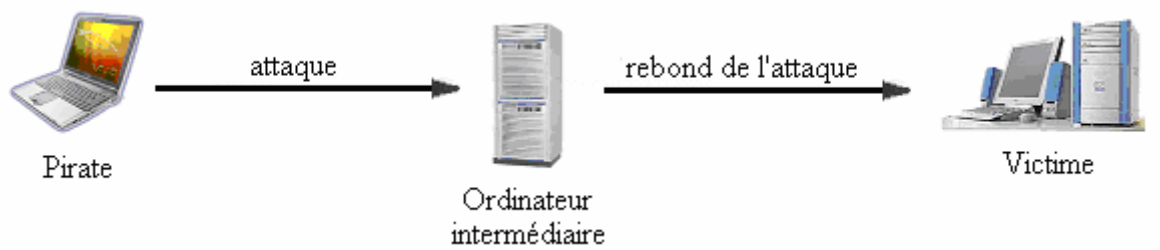
Attaques directes



C'est la plus simple des attaques à réaliser :

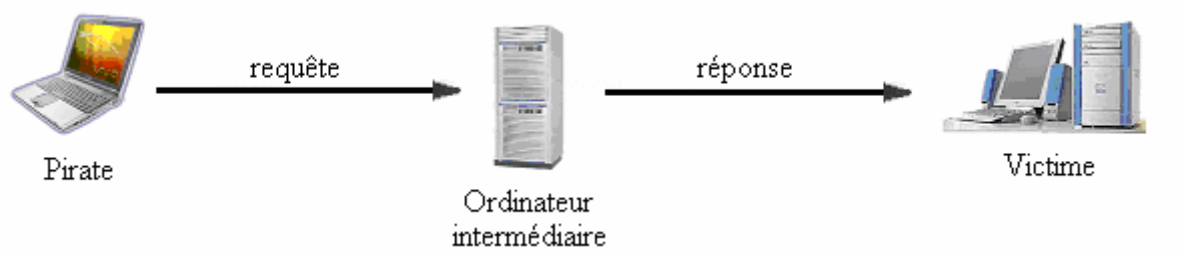
- Le pirate attaque directement sa victime à partir de son ordinateur par des scripts d'attaques faiblement paramétrable
- les programmes de piratage qu'ils utilisent envoient directement les paquets à la victime.
- Dans ce cas, il est possible en général de remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant.

Attaques par rebond



Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les **attaques par rebond** (par opposition aux attaques directes), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer l'adresse IP réelle du pirate et d'utiliser les ressources de la machine servant de rebond.
Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel, car celui-ci se retrouve «complice» contre son gré de l'attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.
Avec le développement des réseaux sans fils, ce type de scénario risque de devenir de plus en plus courant car si le réseau sans fils est mal sécurisé, un pirate situé à proximité peut l'utiliser pour lancer des attaques !

Les attaques indirectes par réponse



Cette attaque est un dérivé de l'attaque par rebond.

- Elle offre les mêmes avantages, du point de vue du pirate.
- Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête.
- Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.

4. Techniques d'attaque
a. Attaque des mots de passe
Introduction
Lorsque vous vous connectez à un système, celui-ci vous demande un identifiant (en anglais login ou username) et un mot de passe (en anglais password) pour y accéder. Ce couple identifiant/mot de passe forme ainsi la clé permettant d'avoir accès au système.
Si l'identifiant est généralement automatiquement attribué par le système ou son administrateur, le choix du mot de passe est souvent laissé libre à l'utilisateur. Ainsi, la plupart des utilisateurs, estimant qu'ils n'ont rien de vraiment secret à protéger, se contentent d'utiliser un mot de passe facile à retenir (par exemple leur identifiant ou leur date de naissance).
Or, si les données sur le compte de l'utilisateur n'ont pas de caractères stratégiques, l'accès au compte de l'utilisateur peut constituer une porte ouverte vers le système tout entier pour tout pirate un tant soit peu expérimenté. En effet, dès lors qu'un pirate obtient un accès à un compte d'une machine, il lui est possible d'élargir son champ d'action en obtenant la liste des utilisateurs autorisés à se connecter à la machine. A l'aide d'outils de génération de mots de passe, le pirate peut essayer un grand nombre de mots de passe générés aléatoirement ou à l'aide d'un dictionnaire (éventuellement une combinaison des deux). S'il trouve par hasard le mot de passe de l'administrateur, il obtient alors toutes les permissions sur la machine ...
De plus, le pirate peut éventuellement obtenir un accès sur le réseau local de la machine, ce qui signifie qu'il peut dresser une cartographie des autres serveurs côtoyant celui sur lequel il a obtenu un accès.

Les mots de passe des utilisateurs représentent donc la première défense contre les attaques envers un système, c'est la raison pour laquelle tout utilisateur se doit de choisir un mot de passe suffisamment compliqué pour qu'il ne puisse pas être deviné.

Méthodes d'attaque
La plupart des systèmes sont configurés de manière à bloquer temporairement le compte d'un utilisateur après un certain nombre de tentatives de connexion infructueuses. Ainsi, un pirate peut difficilement s'infiltrer sur un système de cette façon.
En contrepartie, un pirate peut se servir de se mécanisme d'auto-défense pour bloquer l'ensemble des comptes utilisateurs afin de provoquer un déni de service.
Sur la plupart des systèmes les mots de passe sont stockés de manière chiffrée (« cryptée ») dans un fichier ou une base de données.
Néanmoins, lorsqu'un pirate obtient un accès au système et obtient ce fichier, il lui est possible de tenter de casser le mot de passe d'un utilisateur en particulier ou bien de l'ensemble des comptes utilisateurs.

Attaque par force brute
On appelle ainsi « attaque par force brute » (en anglais « brute force cracking », parfois également attaque exhaustive) le cassage d'un mot de passe en testant tous les mots de passe possibles. Il existe un grand nombre d'outils, pour chaque système d'exploitation, permettant de réaliser ce genre d'opération. Ces outils servent aux administrateurs système à éprouver la solidité des mots de passe de leurs utilisateurs mais leur usage est détourné par les pirates informatiques pour s'introduire dans les systèmes informatiques.

Attaque par dictionnaire
Les outils d'attaque par force brute peuvent demander des heures, voire des jours, de calcul même avec des machines équipées de processeurs puissants. Ainsi, une alternative consiste à effectuer une « attaque par dictionnaire ». En effet, la plupart du temps les utilisateurs choisissent des mots de passe ayant une signification réelle. Avec ce type d'attaques, un tel mot de passe peut être craqué en quelques minutes.

Attaque hybride
Le dernier type d'attaques de ce type, appelées « attaques hybrides », vise particulièrement les mots de passe constitué d'un mot traditionnel et suivi d'une lettre ou d'un chiffre (tel que « reseau2 »). Il s'agit d'une combinaison d'attaque par force brute et d'attaque par dictionnaire.
Il existe enfin des moyens permettant au pirate d'obtenir les mots de passe des utilisateurs :
Les **keyloggers** (littéralement « enregistreurs de touches »), sont des logiciels qui, lorsqu'ils sont installés sur le poste de l'utilisateur, permettent d'enregistrer les frappes de claviers saisies par l'utilisateur. Les systèmes d'exploitation récents possèdent des mémoires tampon protégées permettant de retenir temporairement le mot de passe et accessibles uniquement par le système.
L'ingénierie sociale consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse appeler l'équipe de support en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence ;
L'**espionnage** représente la plus vieille des méthodes. Il suffit en effet parfois à un pirate d'observer les papiers autour de l'écran de l'utilisateur ou sous le clavier afin d'obtenir le mot de passe. Par ailleurs, si le pirate fait partie de l'entourage de la victime, un simple coup d'oeil par dessus son épaule lors de la saisie du mot de passe peut lui permettre de le voir ou de le deviner.

Choix du mot de passe
Il est aisément compréhensible que plus un mot de passe est long, plus il est difficile à casser. D'autre part, un mot de passe constitué uniquement de chiffres sera beaucoup plus simple à casser qu'un mot de passe contenant des lettres :
Un mot de passe de 4 chiffres correspond à 10 000 possibilités (10^4). Si ce chiffre paraît élevé, un ordinateur doté d'une configuration modeste est capable de le casser en quelques minutes. On lui préfèrera un mot de passe de 4 lettres, pour lequel il existe 456972 possibilités (26^4). Dans le même ordre d'idée, un mot de passe mêlant chiffres et lettres, voire également des majuscules et des caractères spéciaux sera encore plus difficile à casser.
Mots de passe à **éviter** :
Votre identifiant, votre nom, votre prénom ou celui d'un proche (conjoint, enfant, etc.) ;
Un mot du dictionnaire ;
Un mot à l'envers (les outils de cassage de mots de passe prennent en compte cette possibilité) ;
Un mot suivi d'un chiffre, de l'année en cours ou d'une année de naissance (par exemple « tri2008 »).

Politique en matière de mot de passe
L'accès au compte d'un seul employé d'une entreprise peut compromettre la sécurité globale de toute l'organisation. Ainsi, toute entreprise souhaitant garantir un niveau de sécurité optimal se doit de mettre en place une réelle politique de sécurité de matière de mots de passe. Il s'agit notamment d'imposer aux employés le choix d'un mot de passe conforme à certaines exigences, par exemple :
Une longueur de mot de passe minimale
La présence de caractères particuliers
Un changement de casse (minuscule et majuscules)
Par ailleurs, il est possible de renforcer cette politique de sécurité en imposant une durée d'expiration des mots de passe, afin d'obliger les utilisateurs à modifier régulièrement leur mot de passe. Cela complique ainsi la tâche des pirates essayant de casser des mots de passe sur la durée. Par ailleurs il s'agit d'un excellent moyen de limiter la durée de vie des mots de passe ayant été cassés.
Enfin, il est recommandé aux administrateurs système d'utiliser des logiciels de cassage de mots de passe en interne sur les mots de passe de leurs utilisateurs afin d'en éprouver la solidité. Ceci doit néanmoins se faire dans le cadre de la politique de sécurité et être écrit noir sur blanc, afin d'avoir l'approbation de la direction et des utilisateurs.

Mots de passe multiples
Il n'est pas sain d'avoir un seul mot de passe, au même titre qu'il ne serait pas sain d'avoir comme code de carte bancaire le même code que pour son téléphone portable et que le digicode en bas de l'immeuble.
Il est donc conseillé de posséder plusieurs mots de passe par catégorie d'usage, en fonction de la confidentialité du secret qu'il protège. Le code d'une carte bancaire devra ainsi être utilisé uniquement pour cet usage. Par contre, le code PIN d'un téléphone portable peut correspondre à celui du cadenas d'une valise.

b. Attaque man in the middle
L'attaque « man in the middle » (littéralement « attaque de l'homme au milieu ») est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties.

La plupart des attaques de type « man in the middle » consistent à écouter le réseau à l'aide d'un outil appelé **sniffer**.

c. Attaque par rejeu

Les attaques par « rejeu » (en anglais « replay attaque ») sont des attaques de type « man in the middle » consistant à intercepter des paquets de données et à les rejouer, c'est-à-dire les retransmettre tels quel (sans aucun déchiffrement) au serveur destinataire.
Ainsi, selon le contexte, le pirate peut bénéficier des droits de l'utilisateur. Imaginons un scénario dans lequel un client transmet un nom d'utilisateur et un mot de passe chiffrés à un serveur afin de s'authentifier. Si un pirate intercepte la communication (grâce à un logiciel d'écoute) et rejoue la séquence, il obtiendra alors les mêmes droits que l'utilisateur. Si le système permet de modifier le mot de passe, il pourra même en mettre un autre, privant ainsi l'utilisateur de son accès.

d. Attaque par déni de service

Une « attaque par déni de service » (en anglais « Denial of Service ») est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.
Les attaques par déni de service sont un fléau pouvant toucher tout serveur d'entreprise ou tout particulier relié à Internet. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur Internet et éventuellement de nuire à leur fonctionnement si leur activité repose sur un système d'information.
D'un point de vue technique, ces attaques ne sont pas très compliquées, mais ne sont pas moins efficaces contre tout type de machine possédant un système d'exploitation Windows (95, 98, NT, 2000, XP, etc.), Linux (Debian, Mandrake, RedHat, Suse, etc.), Unix commercial (HP-UX, AIX, IRIX, Solaris, etc.) ou tout autre système. La plupart des attaques par déni de service exploitent des failles liées à l'implémentation d'un protocole du modèle TCP/IP.
On distingue habituellement deux types de dénis de service :

- Les dénis de service par saturation, consistant à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles ;
- Les dénis de service par exploitation de vulnérabilités, consistant à exploiter une faille du système distant afin de le rendre inutilisable.

Le principe des attaques par déni de service consiste à envoyer des paquets IP ou des données de taille ou de constitution inhabituelle, afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent.
Pour se protéger de ce type d'attaque, il est nécessaire de mener une veille active sur les nouvelles attaques et vulnérabilités et de récupérer sur Internet des correctifs logiciels (patchs) conçus par les éditeurs de logiciels ou certains groupes spécialisés.

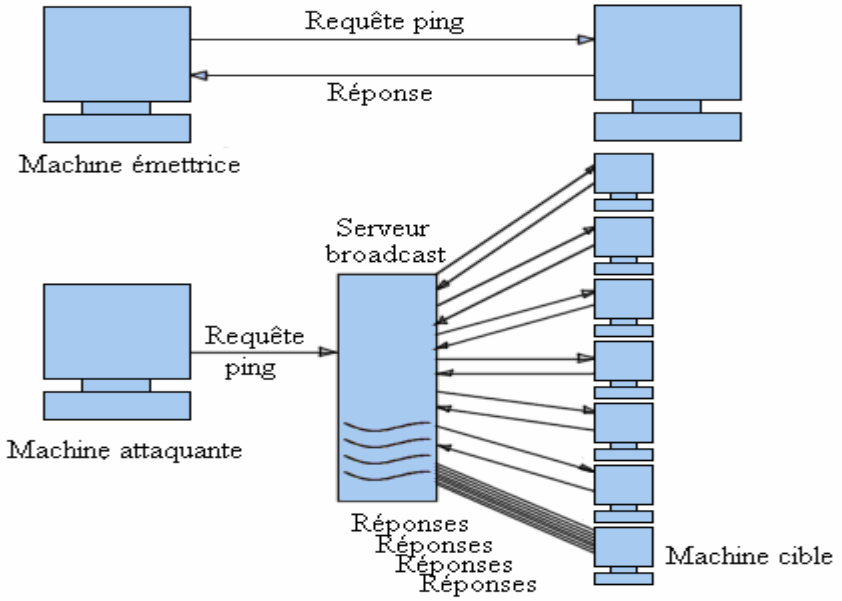
e. Attaque par réflexion (Smurf)

La technique dite « attaque par réflexion » (en anglais « smurf ») est basée sur l'utilisation de serveurs de diffusion (broadcast) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau.

Le scénario d'une telle attaque est le suivant :

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

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

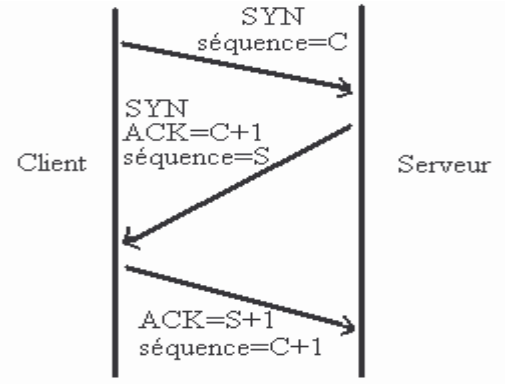


De cette façon l'essentiel du travail de l'attaquant consiste à trouver une liste de serveurs de diffusion et à falsifier l'adresse de réponse afin de les diriger vers la machine cible.

f. Attaque SYN

L'« attaque SYN » (appelée également « TCP/SYN Flooding ») est une attaque réseau par saturation (déni de service) exploitant le mécanisme de poignée de main en trois temps du protocole TCP.

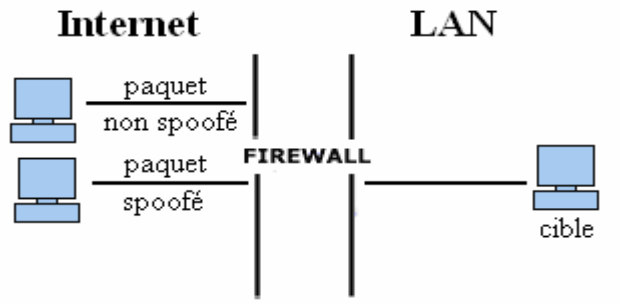
Le mécanisme de poignée de main en trois temps est la manière selon laquelle toute connexion « fiable » à Internet (utilisant le protocole TCP) s'effectue.



Lorsqu'un client établit une connexion à un serveur, le client envoie une requête SYN, le serveur répond alors par un paquet SYN/ACK et enfin le client valide la connexion par un paquet ACK (acknowledgement, qui signifie accord ou remerciement).
Une connexion TCP ne peut s'établir que lorsque ces 3 étapes ont été franchies. L'attaque SYN consiste à envoyer un grand nombre de requêtes SYN à un hôte avec une adresse IP source inexistante ou invalide. Ainsi, il est impossible que la machine cible reçoive un paquet ACK.
Les machines vulnérables aux attaques SYN mettent en file d'attente, dans une structure de données en mémoire, les connexions ainsi ouvertes, et attendent de recevoir un paquet ACK. Il existe un mécanisme d'expiration permettant de rejeter les paquets au bout d'un certain délai. Néanmoins, avec un nombre de paquets SYN très important, si les ressources utilisées par la machine cible pour stocker les requêtes en attente sont épuisées, elle risque d'entrer dans un état instable pouvant conduire à un plantage ou un redémarrage

g. Spoofing IP
L'« usurpation d'adresse IP » (en anglais spoofing IP) est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.
Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

Attaque par usurpation
La technique de l'usurpation d'adresse IP peut permettre à un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le système de filtrage de paquets (pare-feu).
En effet, un système pare-feu (en anglais firewall) fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines internes au réseau.



Ainsi, un paquet spoofé avec l'adresse IP d'une machine interne semblera provenir du réseau interne et sera relayé à la machine cible, tandis qu'un paquet contenant une adresse IP externe sera automatiquement rejeté par le pare-feu.

Modification de l'en-tête TCP
Sur Internet, les informations circulent grâce au protocole IP, qui assure l'encapsulation des données dans des structures appelées paquets (ou plus exactement datagramme IP). Voici la structure d'un datagramme :

Version	Longueur d'en-tête	Type de service	Longueur totale	
Identification			Drapeau	Décalage fragment
Durée de vie		Protocole	Somme de contrôle en-tête	
Adresse IP source				
Adresse IP destination				
Données				

Usurper une adresse IP revient à modifier le champ source afin de simuler un datagramme provenant d'une autre adresse IP. Toutefois, sur Internet, les paquets sont généralement transportés par le protocole TCP, qui assure une transmission dite « fiable ».
Avant d'accepter un paquet, une machine doit auparavant accuser réception de celui-ci auprès de la machine émettrice, et attendre que cette dernière confirme la bonne réception de l'accusé.

Les liens d'approbation
Le protocole TCP est un des principaux protocoles de la couche transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP).
Le protocole TCP permet d'assurer le transfert des données de façon fiable, bien qu'il utilise le protocole IP (qui n'intègre aucun contrôle de livraison de datagramme) grâce à un système d'accusés de réception (ACK) permettant au client et au serveur de s'assurer de la bonne réception mutuelle des données.
Les datagrammes IP encapsulent des paquets TCP (appelés segments) dont voici la structure :

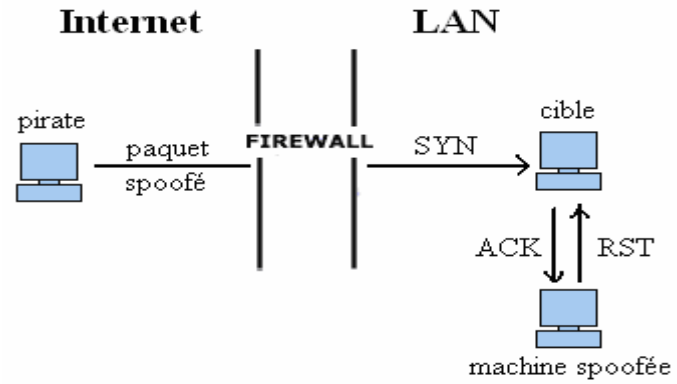
Port Source		Port destination	
Numéro d'ordre			
Numéro d'accusé de réception			
Décalage données	réservée<TD URG <TD ACK <TD PSH <TD RST <TD SYN <TD FIN	Fenêtre	
Somme de contrôle		Pointeur d'urgence	
Options		Remplissage	
Données			

Lors de l'émission d'un segment, un numéro d'ordre (appelé aussi numéro de séquence) est associé, et un échange de segments contenant des champs particuliers (appelés drapeaux, en anglais flags) permet de synchroniser le client et le serveur.
Ce dialogue (appelé poignée de mains en trois temps) permet d'initier la communication, il se déroule en trois temps, comme sa dénomination l'indique:

- Dans un premier temps, la machine émettrice (le client) transmet un segment dont le drapeau SYN est à 1 (pour signaler qu'il s'agit d'un segment de synchronisation), avec un numéro d'ordre N, que l'on appelle numéro d'ordre initial du client.
- Dans un second temps la machine réceptrice (le serveur) reçoit le segment initial provenant du client, puis lui envoie un accusé de réception, c'est-à-dire un segment dont le drapeau ACK est non nul (accusé de réception) et le drapeau SYN est à 1 (car il s'agit là encore d'une synchronisation). Ce segment contient un numéro de séquence égal au numéro d'ordre initial du client. Le champ le plus important de ce segment est le champ accusé de réception (ACK) qui contient le numéro d'ordre initial du client, incrémenté de 1.
- Enfin, le client transmet au serveur un accusé de réception, c'est-à-dire un segment dont le drapeau ACK est non nul, et dont le drapeau SYN est à zéro (il ne s'agit plus d'un segment de synchronisation). Son numéro d'ordre est incrémenté et le numéro d'accusé de réception représente le numéro de séquence initial du serveur incrémenté de 1.
- La machine spoofée va répondre avec un paquet TCP dont le drapeau RST (reset) est non nul, ce qui mettra fin à la connexion.

Annihiler la machine spoofée

Dans le cadre d'une attaque par usurpation d'adresse IP, l'attaquant n'a aucune information en retour car les réponses de la machine cible vont vers une autre machine du réseau (on parle alors d'attaque à l'aveugle).

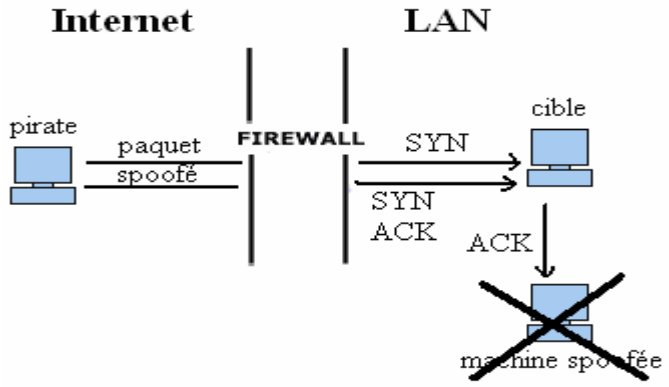


De plus, la machine « spoofée » prive le pirate de toute tentative de connexion, car elle envoie systématiquement un drapeau RST à la machine cible. Le travail du pirate consiste alors à invalider la machine spoofée en la rendant injoignable pendant toute la durée de l'attaque.

Prédire les numéros de séquence

Lorsque la machine spoofée est invalidée, la machine cible attend un paquet contenant l'accusé de réception et le bon numéro de séquence. Tout le travail du pirate consiste alors à « deviner » le numéro de séquence à renvoyer au serveur afin que la relation de confiance soit établie.

Pour cela, les pirates utilisent généralement le « source routing », c'est-à-dire qu'ils utilisent le champ option de l'en-tête IP afin d'indiquer une route de retour spécifique pour le paquet. Ainsi, grâce au sniffing, le pirate sera à même de lire le contenu des trames de retour...



Ainsi, en connaissant le dernier numéro de séquence émis, le pirate établit des statistiques concernant son incrémentation et envoie des accusés de réception jusqu'à obtenir le bon numéro de séquence.

h. Vol de session TCP (hijacking)

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

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

Source-routing

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

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

Attaque à l'aveugle

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

Man in the middle

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

i. Analyseurs réseau (sniffers)

L'analyse de réseau

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

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

Utilisation du sniffer
Un sniffer est un formidable outil permettant d'étudier le trafic d'un réseau. Il sert généralement aux administrateurs pour diagnostiquer les problèmes sur leur réseau ainsi que pour connaître le trafic qui y circule. Ainsi les détecteurs d'intrusion (IDS, pour intrusion detection system) sont basés sur un sniffeur pour la capture des trames, et utilisent une base de données de règles (rules) pour détecter des trames suspectes.
Malheureusement, comme tous les outils d'administration, le sniffer peut également servir à une personne malveillante ayant un accès physique au réseau pour collecter des informations. Ce risque est encore plus important sur les réseaux sans fils car il est difficile de confiner les ondes hertziennes dans un périmètre délimité, si bien que des personnes malveillantes peuvent écouter le trafic en étant simplement dans le voisinage.
La grande majorité des protocoles Internet font transiter les informations en clair, c'est-à-dire de manière non chiffrée. Ainsi, lorsqu'un utilisateur du réseau consulte sa messagerie via le protocole POP ou IMAP, ou bien surfe sur Internet sur des sites dont l'adresse ne commence pas par HTTPS, toutes les informations envoyées ou reçues peuvent être interceptées. C'est comme cela que des sniffers spécifiques ont été mis au point par des pirates afin de récupérer les mots de passe circulant dans le flux réseau.

j. Scanners de vulnérabilités
Un « scanner de vulnérabilité » (parfois appelé « analyseur de réseaux ») est un utilitaire permettant de réaliser un audit de sécurité d'un réseau en effectuant un balayage des ports ouverts (en anglais port scanning) sur une machine donnée ou sur un réseau tout entier. Le balayage se fait grâce à des sondes (requêtes) permettant de déterminer les services fonctionnant sur un hôte distant.
Un tel outil permet de déterminer les risques en matière de sécurité. Il est généralement possible avec ce type d'outil de lancer une analyse sur une plage ou une liste d'adresses IP afin de cartographier entièrement un réseau.
En analysant très finement la structure des paquets TCP/IP reçus, les scanners de sécurité évolués sont parfois capables de déterminer le système d'exploitation de la machine distante ainsi que les versions des applications associées aux ports.

Utilité d'un scanner
Les scanners de sécurité sont des outils très utiles pour les administrateurs système et réseau afin de surveiller la sécurité du parc informatique dont ils ont la charge.
A contrario, cet outil est parfois utilisé par des pirates informatiques afin de déterminer les brèches d'un système.

k. Ingénierie sociale
Le terme d'« ingénierie sociale » (en anglais « social engineering ») désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct.
L'ingénierie sociale est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs en se faisant passer pour une personne de la maison, un technicien, un administrateur, etc.
D'une manière générale les méthodes d'ingénierie sociale se déroulent selon le schéma suivant :

- Une phase d'approche permettant de mettre l'utilisateur en confiance, en se faisant passer pour une personne de sa hiérarchie, de l'entreprise, de son entourage ou pour un client, un fournisseur, etc.

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

L'ingénierie sociale peut prendre plusieurs formes :

- Par téléphone,
- Par courrier électronique,
- Par courrier écrit,
- Par messagerie instantanée…

l. Phishing

Le phishing (contraction des mots anglais « fishing », en français pêche, et « phreaking », désignant le piratage de lignes téléphoniques), traduit parfois en « **hameçonnage** », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.

La technique du phishing est une technique d'« ingénierie sociale » c'est-à-dire consistant à exploiter non pas une faille informatique mais la « faille humaine » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce.

Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.

Dans la mesure où les adresses électroniques sont collectées au hasard sur Internet, le message a généralement peu de sens puisque l'internaute n'est pas client de la banque de laquelle le courrier semble provenir. Mais sur la quantité des messages envoyés il arrive que le destinataire soit effectivement client de la banque.

Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes ou bien des données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.).

Grâce à ces données les pirates sont capables de transférer directement l'argent sur un autre compte ou bien d'obtenir ultérieurement les données nécessaires en utilisant intelligemment les données personnelles ainsi collectées.

m. Attaques sur différents protocoles

Cette partie décrit les failles intrinsèques de différents protocoles. Intrinsèques par le fait qu'elles ne sont pas liées à une faille applicative du client ou du serveur gérant ce protocole, mais plutôt à sa conception.

i. DHCP

Le protocole DHCP est utilisé pour délivrer dynamiquement une adresse IP unique pour chaque machine le demandant sur le réseau interne. En clair, si un client interne veut obtenir une adresse IP pour bénéficier des services réseau, il envoie un message DHCP à tout le réseau (broadcast) pour trouver le serveur DHCP. Le serveur DHCP répondra en lui envoyant tous les paramètres de configuration réseau.

Ce service permet «d'alléger» la gestion du réseau en évitant d'avoir des configurations statiques à maintenir sur chaque machine. Malheureusement, le protocole DHCP comporte diverses failles que nous allons vous présenter.

Attaque par épuisement de ressources
Comme il l'a été décrit, un serveur DHCP possède un stock d'adresses IP qu'il distribue aux différents clients. Ce stock est bien sûr limité. Il y aura seulement un nombre défini de clients pouvant disposer des différentes adresses IP en même temps. Si le serveur est bien administré avec une liste «fermée» de correspondances entre adresses MAC et IP aucune attaque par épuisement n'est possible.
Si le service est mal administré ; c'est à dire que les correspondances entre adresses MAC et IP se font dynamiquement à partir d'une plage d'adresses IP vacantes, le scénario suivant est possible : si un pirate génère un grand nombre de requêtes DHCP semblant venir d'un grand nombre de clients différents, le serveur épuisera vite son stock d'adresses. Les «vrais» clients ne pourront donc plus obtenir d'adresse IP : le trafic réseau sera paralysé.

Faux serveurs DHCP
Cette attaque vient en complément de la première. Si un pirate a réussi à saturer un serveur DHCP par épuisement de ressources, il peut très bien en activer un autre à la place. Ainsi il pourra ainsi contrôler tout le trafic réseau.

ii. DNS
Le protocole DNS assure la correspondance entre le nom d'une machine et son adresse IP. Un serveur DNS est en écoute par défaut sur le UDP port 53. Les attaques décrites ici concernent les faiblesses du protocole DNS.

Le DNS ID spoofing
C'est la première attaque que nous allons décrire. Elle aboutit à un détournement de flux entre deux machines à l'avantage du pirate.
Imaginons qu'un client **A** veuille établir une connexion avec une machine **B**. La machine **A** connaît le nom de la machine **B** mais pas son adresse IP, ce qui lui empêche pouvoir communiquer avec.
La machine **A** va donc envoyer une requête au serveur DNS du réseau de **B** pour connaître l'adresse IP de **B**, cette requête sera identifiée par un numéro d'identification (ID).
Le serveur répond à cette requête en fournissant l'adresse IP de B et en utilisant le même numéro d'ID. Ce numéro a une valeur comprise entre 0 et 65535.
Le DNS ID spoofing a pour but de d'envoyer une fausse réponse à une requête DNS avant le serveur DNS. De cette façon, le pirate peut rediriger vers lui le trafic à destination d'une machine qu'il l'intéresse.
Dans notre exemple, un pirate **C** doit répondre à **A** avant le serveur DNS (D) du réseau de **B**.
Ainsi, il envoie à **A** son adresse IP associée au nom de la machine **B**. **A** communiquera alors avec le pirate **C** au lieu de la machine **B**.
Néanmoins, pour implémenter cette attaque, le pirate doit connaître l'ID de requête DNS. Pour cela, il peut utiliser un sniffer s'il est sur le même réseau, soit prédire les numéros d'ID par l'envoi de plusieurs requêtes et l'analyse des réponses.

Le DNS cache poisoning

Pour gagner du temps dans la gestion des requêtes, le serveur DNS possède un cache temporaire contenant les correspondances adresses IP - noms de machine. En effet, un serveur DNS n'a que la table de correspondance des machines du réseau sur lequel il a autorité. Pour des machines distantes, il doit interroger d'autres serveurs DNS. Pour éviter de les interroger à chaque requête, il garde en mémoire (dans un cache), le résultat des précédentes requêtes.
L'objectif du pirate est d'empoisonner ce cache avec de fausses informations. Pour cela, il doit avoir un nom de domaine sous contrôle et son serveur DNS.
Imaginons qu'un pirate (A) possède le nom de domaine attaquant.com, et son serveur DNS (C) et qu'il veuille empoisonner le cache du serveur DNS (B) du réseau cible.net.
Le pirate envoie une requête au serveur DNS (B) du réseau cible.net demandant la résolution du nom de domaine attaquant.com.
Le serveur DNS (B) de cible.net va donc envoyer une requête sur le serveur DNS (C) de l'attaquant (c'est lui qui a autorité sur le domaine attaquant.com). Celui-ci répondra et joindra des informations additionnelles falsifiées par le pirate (un nom de machine (D) associé à l'adresse IP (A) du pirate). Ces informations seront mises en cache sur le serveur DNS (B) de cible.net. Si un client quelconque (E) demande l'adresse IP pour le nom de la machine (D), il recevra l'adresse du pirate (A) en retour.

iii. FTP

FTP (File Transfert Protocol, en écoute par défaut sur les ports 20 et 21) est le service utilisé pour assurer le transfert de fichiers. Il y a deux types de serveurs FTP : les serveurs FTP avec authentification par mots de passe et les serveurs anonymes. Pour les premiers, le client désirant se connecter devra fournir un login accompagné d'un mot de passe pour authentification. Dans le cas du serveur FTP anonyme, tout le monde peut s'y connecter librement.
Le premier défaut du protocole FTP est de ne pas encrypter les mots de passe lors de leur transit sur le réseau. Les mots de passe associés aux logins circulent en clair à la merci des sniffers.

Voici l'exemple d'une interception par un sniffer d'une authentification FTP :
Le logiciel utilisé est « tcpdump ».

```
22:10:39.528557 192.168.1.3.1027 ¿ 192.168.1.4.ftp: P 1:12(11) ack 47
win 5840 ¡nop,nop,timestamp 441749 100314¿ (DF) [tos 0x10]
0x0000 4510 003f 88d6 4000 4006 2e7b c0a8 0103 E.. ?..@.@.....
0x0010 c0a8 0104 0403 0015 e351 3262 8d6a dd80 .........Q2b.j..
0x0020 8018 16d0 68da 0000 0101 080a 0006 bd95 ....h...........
0x0030 0001 87da 5553 4552 2061 6c65 780d 0a00 ....0,1,0USER.adil...
22:10:57.746008 192.168.1.3.1027 ¿ 192.168.1.4.ftp: P 12:23(11) ack 80
win 5840 ¡nop,nop,timestamp 443571 101048¿ (DF) [tos 0x10]
0x0000 4510 003f 88d8 4000 4006 2e79 c0a8 0103 E.. ?..@.@..y....
0x0010 c0a8 0104 0403 0015 e351 326d 8d6a dda1 .........Q2m.j..
0x0020 8018 16d0 5ba1 0000 0101 080a 0006 c4b3 ....[...........
0x0030 0001 8ab8 5041 5353 2074 6f74 6f0d 0a00 ....0,1,0PASS.soso...
```

On peut voir facilement que l'utilisateur adil a le mot de passe soso.

Le serveur FTP anonyme

Le serveur FTP anonyme pose de plus gros problèmes. Le premier est qu'une mauvaise gestion des droits d'accès peut s'avérer être une erreur fatale. Laisser trop de répertoires en droit d'écriture et/ou d'exécution est plus que dangereux pour la sûreté du système. Le pirate pourrait y installer ou y exécuter des codes malveillants lui permettant d'accroître son pouvoir sur la machine.

Boucing attack - Attaque par rebonds
Les serveurs FTP anonymes peuvent être sujets à des attaques par rebonds. Ces attaques consistent à utiliser un serveur FTP anonyme comme relais pour se connecter à d'autres serveurs FTP. Imaginons qu'un pirate se voit refuser l'accès par un serveur FTP dont l'accès est alloué à seulement un certain groupe d'adresses IP. Imaginons que le pirate ne fait pas partie de ce groupe, mais qu'un serveur FTP anonyme y appartienne. Le pirate peut très bien se connecter sur le serveur FTP anonyme, utiliser les commandes assurant la connexion sur le serveur FTP protégé et y récupérer des fichiers.

iv. HTTP
Un serveur HTTP est en écoute sur le port 80. Le protocole HTTP est sûrement le plus utilisé sur le web pour les pages html. Ce protocole ne comporte pas de failles intrinsèques majeures. Par contre, les applications assurant son traitement sont souvent bourrées de failles. Cela vient du fait que le web devient de plus en plus demandeur en terme de convivialité et cela génère une complexité plus grande des applications, d'où un risque de failles plus important.

Les serveurs trop bavards
Parfois, les bannières des serveurs web sont trop explicites. Exemple sur un serveur Apache :

```
[root@nowhere /root]# telnet 127.0.0.1 80
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Date: Sun, 04 Jan 2004 15:07:06 GMT
Server: Apache/1.3.29 (Debian GNU/Linux)
Last-Modified: Sat, 24 Nov 2001 16:48:12 GMT
ETag: "17082-100e-3bffcf4c"
Accept-Ranges: bytes
Content-Length: 4110
Connection: close
Content-Type: text/html; charset=iso-8859-1
Connection closed by foreign host.
```

Lors de l'envoi de la commande **HEAD / HTTP/1.0**, trop d'informations sont données.
Les pages d'erreurs (404 : page non trouvée) peuvent aussi contenir des informations sur le système.

Vulnérabilités liées aux applications web
La complexité des serveurs ou des navigateurs (clients) web pose de gros problèmes de sécurité. Ces applications sont vulnérables à de nombreux bugs. Chaque application a son type de faille.
Netscape par exemple devient vulnérable lors du traitement de certaines chaînes de caractères. Cela peut permettre de remonter toute l'arborescence des fichiers du serveur. Les serveurs IIS peuvent renvoyer un shell système pour un envoi de commandes particulières.
Les langages comme Javascript, Perl, PHP, ASP pour la réalisation de scripts peuvent se révéler dangereux. L'origine d'une faille dans une application web peut apparaître à cause de deux problèmes. Le premier est la fiabilité de la conception du script, le second est la fiabilité des fonctions utilisées. Si un script est mal conçu, il peut être la source de nombreuses failles. De même, si sa conception est bonne mais qu'il utilise des fonctions boguées, il peut se révéler encore plus dangereux.

III. Mesures pour la protection

1. Protection des données

Il existe plusieurs mesures pour protéger les données dans un système informatique on cite surtout la technologie RAID et la cryptographie.

a. RAID

La technologie RAID (acronyme de Redundant Array of Inexpensive Disks, parfois Redundant Array of Independent Disks, traduisez Ensemble redondant de disques indépendants) permet de constituer une unité de stockage à partir de plusieurs disques durs. L'unité ainsi créée (appelée **grappe**) a donc une grande tolérance aux pannes (haute disponibilité), ou bien une plus grande capacité/vitesse d'écriture. La répartition des données sur plusieurs disques durs permet donc d'en augmenter la sécurité et de fiabiliser les services associés.

Les disques assemblés selon la technologie RAID peuvent être utilisés de différentes façons, appelées **Niveaux RAID**. L'Université de Californie en a défini 5, auxquels ont été ajoutés les niveaux 0 et 6. Chacun d'entre-eux décrit la manière de laquelle les données sont réparties sur les disques :

- **Niveau 0**: appelé striping
- **Niveau 1**: appelé mirroring, shadowing ou duplexing
- **Niveau 2**: appelé striping with parity (obsolète)
- **Niveau 3**: appelé disk array with bit-interleaved data
- **Niveau 4**: appelé disk array with block-interleaved data
- **Niveau 5**: appelé disk array with block-interleaved distributed parity
- **Niveau 6**: appelé disk array with block-interleaved distributed parity

Niveau 0

Le niveau RAID-0, appelé **striping** consiste à stocker les données en les répartissant sur l'ensemble des disques de la grappe. De cette façon, il n'y a pas de redondance, on ne peut donc pas parler de tolérance aux pannes. En effet en cas de défaillance de l'un des disques, l'intégralité des données réparties sur les disques sera perdue.

Toutefois, étant donné que chaque disque de la grappe a son propre contrôleur, cela constitue une solution offrant une vitesse de transfert élevée.

Le RAID 0 consiste ainsi en la juxtaposition logique (agrégation) de plusieurs disques durs physiques. En mode RAID-0 les données sont écrites par "bandes" (en anglais stripes) :

Disque 1	**Disque 2**	**Disque 3**
Bande 1	Bande 2	Bande 3
Bande 4	Bande 5	Bande 6
Bande 7	Bande 8	Bande 9

On parle de facteur d'entrelacement pour caractériser la taille relative des fragments (bandes) stockés sur chaque unité physique. Le débit de transfert moyen dépend de ce facteur (plus petite est chaque bande, meilleur est le débit).

Si un des éléments de la grappe est plus grand que les autres, le système de remplissage par bande se trouvera bloqué lorsque le plus petit des disques sera rempli. La taille finale est ainsi égale au double de la capacité du plus petit des deux disques :

- deux disques de 20 Go donneront un disque logique de 40 Go.
- un disque de 10 Go utilisé conjointement avec un disque de 27 Go permettra d'obtenir un disque logique de 20 Go (17 Go du second disque seront alors inutilisés).

Remarque : Il est recommandé d'utiliser des disques de même taille pour faire du RAID-0 car dans le cas contraire le disque de plus grande capacité ne sera pas pleinement exploité.

Niveau 1
Le niveau 1 a pour but de dupliquer l'information à stocker sur plusieurs disques, on parle donc de mirroring, ou shadowing pour désigner ce procédé.

Disque1	Disque2	Disque3
Bande 1	Bande 1	Bande 1
Bande 2	Bande 2	Bande 2
Bande 3	Bande 3	Bande 3

On obtient ainsi une plus grande sécurité des données, car si l'un des disques tombe en panne, les données sont sauvegardées sur l'autre. D'autre part, la lecture peut être beaucoup plus rapide lorsque les deux disques sont en fonctionnement. Enfin, étant donné que chaque disque possède son propre contrôleur, le serveur peut continuer à fonctionner même lorsque l'un des disques tombe en panne, au même titre qu'un camion pourra continuer à rouler si un de ses pneus crève, car il en a plusieurs sur chaque essieu...
En contrepartie la technologie RAID1 est très onéreuse étant donné que seule la moitié de la capacité de stockage n'est effectivement utilisée.

Niveau 2
Le niveau RAID-2 est désormais obsolète, car il propose un contrôle d'erreur par code de Hamming (codes **ECC** - Error Correction Code), or ce dernier est désormais directement intégré dans les contrôleurs de disques durs.
Cette technologie consiste à stocker les données selon le même principe qu'avec le RAID-0 mais en écrivant sur une unité distincte les bits de contrôle ECC (généralement 3 disques ECC sont utilisés pour 4 disques de données).
La technologie RAID 2 offre de piètres performances mais un niveau de sécurité élevé.

Niveau 3
Le niveau 3 propose de stocker les données sous forme d'octets sur chaque disque et de dédier un des disques au stockage d'un bit de parité.

Disque 1	Disque 2	Disque 3	Disque 4
Octet 1	Octet 2	Octet 3	Parité 1+2+3
Octet 4	Octet 5	Octet 6	Parité 4+5+6
Octet 7	Octet 8	Octet 9	Parité 7+8+9

De cette manière, si l'un des disques venait à défaillir, il serait possible de reconstituer l'information à partir des autres disques. Après "reconstitution" le contenu du disque défaillant est de nouveau intègre. Par contre, si deux disques venaient à tomber en panne simultanément, il serait alors impossible de remédier à la perte de données.

Niveau 4
Le niveau 4 est très proche du niveau 3. La différence se trouve au niveau de la parité, qui est faite sur un secteur (appelé bloc) et non au niveau du bit, et qui est stockée sur un disque dédié. C'est-à-dire plus précisément que la valeur du facteur d'entrelacement est différente par rapport au RAID 3.

Disque 1	Disque 2	Disque 3	Disque 4
Bloc 1	Bloc 2	Bloc 3	Parité 1+2+3
Bloc 4	Bloc 5	Bloc 6	Parité 4+5+6
Bloc 7	Bloc 8	Bloc 9	Parité 7+8+9

Ainsi, pour lire un nombre de blocs réduits, le système n'a pas à accéder à de multiples lecteurs physiques, mais uniquement à ceux sur lesquels les données sont effectivement stockées. En contrepartie le disque hébergeant les données de contrôle doit avoir un temps d'accès égal à la somme des temps d'accès des autres disques pour ne pas limiter les performances de l'ensemble.

Niveau 5
Le niveau 5 est similaire au niveau 4, c'est-à-dire que la parité est calculée au niveau d'un secteur, mais répartie sur l'ensemble des disques de la grappe.

Disque 1	Disque 2	Disque 3	Disque 4
Bloc 1	Bloc 2	Bloc 3	Parité 1+2+3
Bloc 4	Parité 4+5+6	Bloc 5	Bloc 6
Parité 7+8+9	Bloc 7	Bloc 8	Bloc 9

De cette façon, RAID 5 améliore grandement l'accès aux données (aussi bien en lecture qu'en écriture) car l'accès aux bits de parité est réparti sur les différents disques de la grappe.
Le mode RAID-5 permet d'obtenir des performances très proches de celles obtenues en RAID-0, tout en assurant une tolérance aux pannes élevée, c'est la raison pour laquelle c'est un des modes RAID les plus intéressants en terme de performance et de fiabilité.
Remarque : L'espace disque utile sur une grappe de n disques étant égal à n-1 disques, il est intéressant d'avoir un grand nombre de disques pour "rentabiliser" le RAID-5.

Niveau 6
Le niveau 6 a été ajouté aux niveaux définis par Berkeley. Il définit l'utilisation de 2 fonctions de parité, et donc leur stockage sur deux disques dédiés. Ce niveau permet ainsi d'assurer la redondance en cas d'avarie simultanée de deux disques. Cela signifie qu'il faut au moins 4 disques pour mettre en oeuvre un système RAID-6.

Comparaison
Les solutions RAID généralement retenues sont le RAID de niveau 1 et le RAID de niveau 5.
Le choix d'une solution RAID est lié à trois critères :

- **la sécurité** : RAID 1 et 5 offrent tous les deux un niveau de sécurité élevé, toutefois la méthode de reconstruction des disques varie entre les deux solutions. En cas de panne du système, RAID 5 reconstruit le disque manquant à partir des informations stockées sur les autres disques, tandis que RAID 1 opère une copie disque à disque.

- **Les performances** : RAID 1 offre de meilleures performances que RAID 5 en lecture, mais souffre lors d'importantes opérations d'écriture.
- **Le coût** : le coût est directement lié à la capacité de stockage devant être mise en oeuvre pour avoir une certaine capacité effective. La solution RAID 5 offre un volume utile représentant 80 à 90% du volume alloué (le reste servant évidemment au contrôle d'erreur). La solution RAID 1 n'offre par contre qu'un volume disponible représentant 50 % du volume total (étant donné que les informations sont dupliquées).

Mise en place d'une solution RAID :
Il existe plusieurs façons différentes de mettre en place une solution RAID sur un serveur :
- **de façon logicielle** : il s'agit généralement d'un driver au niveau du système d'exploitation de l'ordinateur capable de créer un seul volume logique avec plusieurs disques (SCSI ou IDE).
- **de façon matérielle**
    - **avec des matériels DASD** (Direct Access Stockage Device) : il s'agit d'unités de stockage externes pourvues d'une alimentation propre. De plus ces matériels sont dotés de connecteurs permettant l'échange de disques à chaud (on dit généralement que ce type de disque est hot swappable). Ce matériel gère lui-même ses disques, si bien qu'il est reconnu comme un disque SCSI standard.
    - **avec des contrôleurs de disques RAID** : il s'agit de cartes s'enfichant dans des slots PCI ou ISA et permettant de contrôler plusieurs disques durs.

b. Cryptographie
La cryptographie est une des disciplines de la cryptologie, s'attachant à protéger des messages (assurant confidentialité et/ou authenticité), en s'aidant souvent de secrets ou clés.
Elle est utilisée depuis l'antiquité, mais certaines de ses méthodes les plus importantes, comme la cryptographie asymétrique, n'ont que quelques dizaines d'années d'existence.

i.Vocabulaire
- **chiffrement et déchiffrement** : le chiffrement est la transformation à l'aide d'une clé de chiffrement d'un message en clair en un message incompréhensible si on ne dispose pas d'une clé de déchiffrement
- **chiffre** : anciennement code secret, par extension, algorithme utilisé pour le chiffrement
- **cryptogramme** : message chiffré
- **décrypter** : retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement ou même retrouver la clé de déchiffrement (terme que ne possède pas les anglophones, qui eux cassent des codes secrets)
- **cryptographie** : étymologiquement écriture secrète, est devenue par extension l'étude de cet art. C'est donc aujourd'hui la science visant à créer des chiffres
- **cryptanalyse** : science analysant les cryptogrammes en vue de les casser

ii. Algorithmes de chiffrement faibles (cassables facilement)
Les premiers algorithmes utilisés pour le chiffrement d'une information étaient assez rudimentaires dans leur ensemble. Ils consistaient notamment au remplacement de caractères par d'autres. La confidentialité de l'algorithme de chiffrement est donc la pierre angulaire de ce système pour éviter un cassage rapide.
Exemple :
- ROT13 (rotation de 13 caractères, sans clé)
- Chiffre de Vigenère (chiffrement polyalphabétique)

iii. Algorithmes de cryptographie symétrique (à clé secrète)

Les algorithmes de chiffrement symétrique se basent sur une même clé (ou presque) pour chiffrer et déchiffrer un message. Le problème de cette technique est qu'il faut que toutes les clés soient parfaitement confidentielles. Et lorsqu'un grand nombre de personnes désirent communiquer ensemble, le nombre de clés augmente de façon importante (une pour chaque couple communicant). Ce qui pose des problèmes de gestions des clés (pour un groupe de n personnes utilisant un cryptosystème à clés secrètes, il est nécessaire de distribuer $n \times (n-1) / 2$ clés).

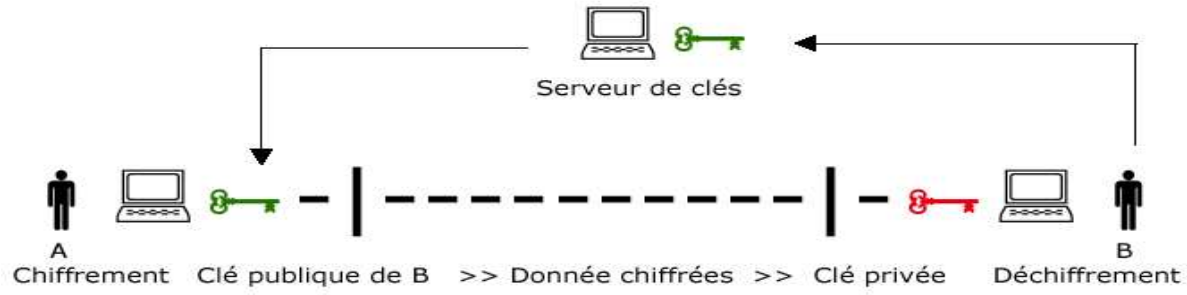
Quelques algorithmes de chiffrement symétrique très utilisés :

- DES (Data Encryption System)
- AES (Advanced Encryption System)
- RC4

iv. Algorithmes de cryptographie asymétrique (à clé publique et privée)

Pour résoudre en partie le problème de la gestion des clés, la cryptographie asymétrique a été mise au point dans les années 1970. Elle se base sur le principe de deux clés :

- une **publique**, permettant le chiffrement
- une **privée**, permettant le déchiffrement



Comme son nom l'indique, la clé publique est mise à la disposition de quiconque désire chiffrer un message. Ce dernier ne pourra être déchiffré qu'avec la clé privée, qui elle doit être confidentielle.

Quelques algorithmes de cryptographie asymétrique très utilisés :

- RSA (Rivest Shamir Adleman)
- DSA (Digital Signature Algorithm)

v. Exemple de cryptosystèmes

Le chiffrement de Vigenère

Le chiffrement de Vigenère est un cryptosystème symétrique, ce qui signifie qu'il utilise la même clé pour le chiffrement et le déchiffrement. Le chiffrement de Vigenère ressemble beaucoup au chiffrement de César, à la différence près qu'il utilise une clef plus longue afin de pallier le principal problème du chiffrement de César: le fait qu'une lettre puisse être codée d'une seule façon. Pour cela on utilise un mot clef au lieu d'un simple caractère. On associe dans un premier temps à chaque lettre un chiffre correspondant.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Il consiste à coder un texte avec un mot en ajoutant à chacune de ses lettres la lettre d'un autre mot appelé clé. La clé est ajoutée indéfiniment en vis-à-vis avec le texte à chiffrer, puis le code ASCII de chacune des lettres de la clé est ajouté au texte à crypter.

Par exemple le texte "rendezvousamidi" avec la clé "bonjour" sera codé de la manière suivante:

Texte original:

r	e	n	d	e	z	v	o	u	s	a	m	i	d	i
114	101	110	100	101	122	118	111	117	115	97	109	105	100	105

Clé:

b	o	n	j	o	u	r
98	111	110	106	111	117	114

Texte crypté

r+b	e+o	n+n	d+j	e+o	z+u	v+r	o+b	u+o	s+n	a+j	m+o	i+u	d+r	i+b
114 + 98	101 + 111	110 + 110	100 + 106	101 + 111	122 + 117	118 + 114	111 + 98	117 + 111	115 + 110	97 + 106	109 + 111	105 + 117	100 + 114	105 + 98

Pour déchiffrer ce message il suffit d'avoir la clé secrète et faire le déchiffrement inverse, à l'aide d'une soustraction.

Bien que ce chiffrement soit beaucoup plus sûr que le chiffrement de César, il peut encore être facilement cassé. En effet, lorsque les messages sont beaucoup plus longs que la clef, il est possible de repérer la longueur de la clef et d'utiliser pour chaque séquence de la longueur de la clef la méthode consistant à calculer la fréquence d'apparition des lettres, permettant de déterminer un à un les caractères de la clef...

Pour éviter ce problème, une solution consiste à utiliser une clef dont la taille est proche de celle du texte afin de rendre impossible une étude statistique du texte crypté. Ce type de système de chiffrement est appelé système à clé jetable. Le problème de ce type de méthode est la longueur de la clé de cryptage (plus le texte à crypter est long, plus la clef doit être volumineuse), qui empêche sa mémorisation et implique une probabilité d'erreur dans la clé beaucoup plus grande (une seule erreur rend le texte indéchiffrable...).

RSA

Le fonctionnement du cryptosystème RSA est basé sur la difficulté de factoriser de grands entiers.

Soit deux nombres premiers p et q, et d un entier tel que d soit premier avec $(p-1)\times(q-1)$. Le triplet (p,q,d) constitue ainsi la clé privée.

La clé publique est alors le doublet (n,e) créé à l'aide de la clé privée par les transformations suivantes :

$n = p \times q$

$e = 1/d \bmod((p-1)(q-1))$

Soit M, le message à envoyer. Il faut que le message M soit premier avec la clé n. En effet, le déchiffrement repose sur le théorème d'Euler stipulant que si M et n sont premiers entre eux, alors :

$M^{phi(n)} = 1 \bmod(n)$

Phi(n) étant l'indicateur d'Euler, et valant dans le cas présent $(p-1) \times (q-1)$.

Il est donc nécessaire que M ne soit pas un multiple de p, de q, ou de n. Une solution consiste à découper le message M en morceaux M_i tels que le nombre de chiffres de chaque M_i soit strictement inférieur à celui de p et de q. Cela suppose donc que p et q soient grand, ce qui est le cas en pratique puisque tout le principe de RSA réside dans la difficulté à trouver dans un temps raisonnable p et q connaissant n, ce qui suppose p et q grands.

Exemple :
Création de la paire de clés:
Soient deux nombres premiers au hasard: p = 29, q = 37, on calcule n = pq = 29 × 37 = 1073.
On doit choisir e au hasard tel que e n'ai aucun facteur en commun avec (p-1)(q-1) :
(p-1)(q-1) = (29-1)(37-1) = 1008
On prend e = 71
On choisit d tel que 71×d mod 1008 = 1, on trouve d = 1079.
On a maintenant les clés :
La clé publique est (e,n) = (71,1073) (=clé de chiffrement)
La clé privée est (d,n) = (1079,1073) (=clé de déchiffrement)

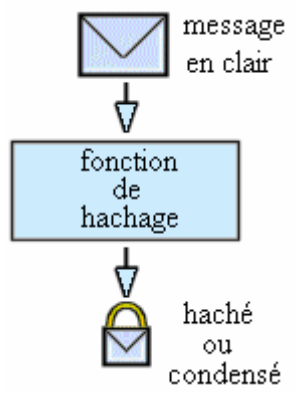
Chiffrement du message 'HELLO' :
On prend le code ASCII de chaque caractère et on les met bout à bout:
M = 7269767679
Il faut découper le message en blocs qui comportent moins de chiffres que n.
n comporte 4 chiffres, on découpe notre message en blocs de 3 chiffres:
726 976 767 900 (on complète avec des zéros)
On chiffre chacun de ces blocs :
726^71 mod 1073 = 436
976^71 mod 1073 = 822
767^71 mod 1073 = 825
900^71 mod 1073 = 552
Le message chiffré est 436 822 825 552.
On peut le déchiffrer avec d:
436^1079 mod 1073 = 726
822^1079 mod 1073 = 976
825^1079 mod 1073 = 767
552^1079 mod 1073 = 900
C'est à dire la suite de chiffre 726976767900.
On retrouve notre message en clair 72 69 76 76 79 : 'HELLO' !

vi. La signature électronique

Le paradigme de signature électronique (appelé aussi signature numérique) est un procédé permettant de garantir l'authenticité de l'expéditeur (fonction d'authentification) et de vérifier l'intégrité du message reçu.
La signature électronique assure également une fonction de non-répudiation, c'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message (autrement dit elle empêche l'expéditeur de nier avoir expédié le message).

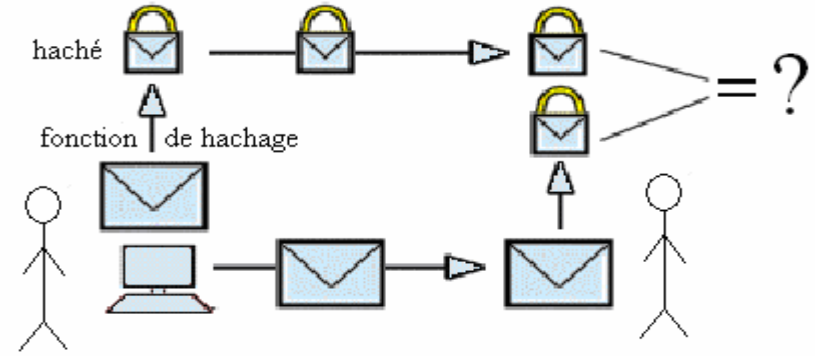
Qu'est-ce qu'une fonction de hachage ?

Une fonction de hachage (parfois appelée fonction de condensation) est une fonction permettant d'obtenir un condensé (appelé aussi condensat ou haché ou en anglais message digest) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense. La fonction de hachage doit être telle qu'elle associe un et un seul haché à un texte en clair (cela signifie que la moindre modification du document entraîne la modification de son haché). D'autre part, il doit s'agir d'une fonction à sens unique (one-way function) afin qu'il soit impossible de retrouver le message original à partir du condensé. S'il existe un moyen de retrouver le message en clair à partir du haché, la fonction de hachage est dite « à brèche secrète ».



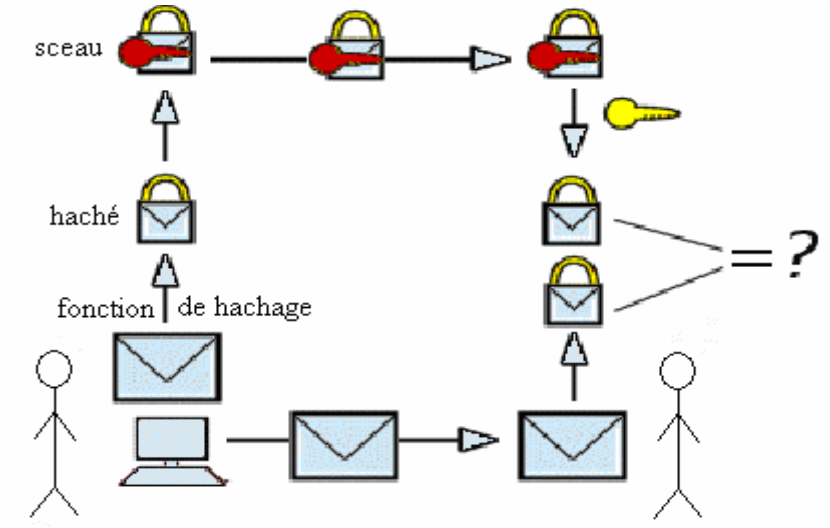
Ainsi, le haché représente en quelque sorte l'empreinte digitale (en anglais finger print) du document.
Les algorithmes de hachage les plus utilisés actuellement sont :
MD5 (MD signifiant Message Digest). Développé par Rivest en 1991, MD5 crée une empreinte digitale de 128 bits à partir d'un texte de taille arbitraire en le traitant par blocs de 512 bits. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du condensé du document permettant de vérifier l'intégrité de ce dernier.
SHA (pour Secure Hash Algorithm, pouvant être traduit par Algorithme de hachage sécurisé) crée des empreintes d'une longueur de 160 bits. SHA-1 est une version améliorée de SHA datant de 1994 et produisant une empreinte de 160 bits à partir d'un message d'une longueur maximale de 2^{64} bits en le traitant par blocs de 512 bits.

Vérification d'intégrité
En expédiant un message accompagné de son haché, il est possible de garantir l'intégrité d'un message, c'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré (intentionnellement ou de manière fortuite) durant la communication.



Lors de la réception du message, il suffit au destinataire de calculer le haché du message reçu et de le comparer avec le haché accompagnant le document. Si le message (ou le haché) a été falsifié durant la communication, les deux empreintes ne correspondront pas.

Le scellement des données
L'utilisation d'une fonction de hachage permet de vérifier que l'empreinte correspond bien au message reçu, mais rien ne prouve que le message a bien été envoyé par celui que l'on croit être l'expéditeur.
Ainsi, pour garantir l'authentification du message, il suffit à l'expéditeur de chiffrer (on dit généralement signer) le condensé à l'aide de sa clé privée (le haché signé est appelé sceau) et d'envoyer le sceau au destinataire.



A réception du message, il suffit au destinataire de déchiffrer le sceau avec la clé publique de l'expéditeur, puis de comparer le haché obtenu avec la fonction de hachage au haché reçu en pièce jointe. Ce mécanisme de création de sceau est appelé scellement.

vii. Les certificats

Introduction

Les algorithmes de chiffrement asymétrique sont basés sur le partage entre les différents utilisateurs d'une clé publique. Généralement le partage de cette clé se fait au travers d'un annuaire électronique ou bien d'un site web.

Toutefois ce mode de partage a une grande lacune : **rien ne garantit que la clé est bien celle de l'utilisateur a qui elle est associée**. En effet un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique. Ainsi, le pirate sera en mesure de déchiffrer tous les messages ayant été chiffrés avec la clé présente dans l'annuaire.

Ainsi un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée **CA** pour Certification Authority).

L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

Qu'est-ce qu'un certificat ?

Les certificats sont des petits fichiers divisés en deux parties :

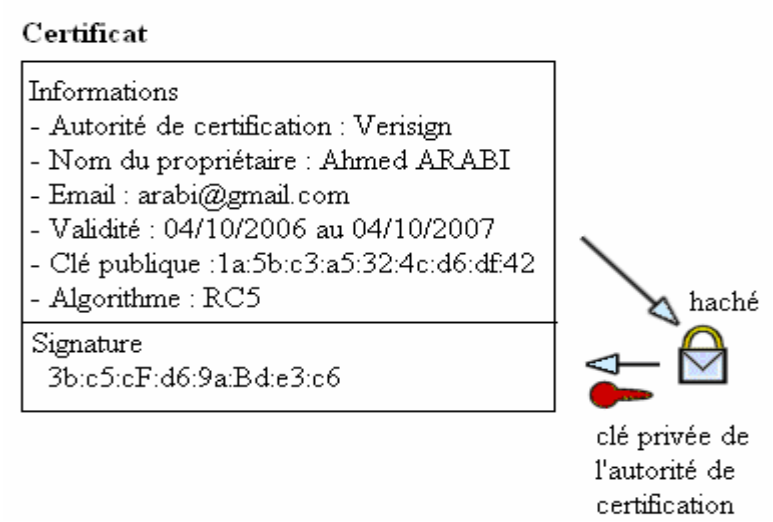
- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification

La structure des certificats est normalisée par le standard X.509 de l'UIT, qui définit les informations contenues dans le certificat :

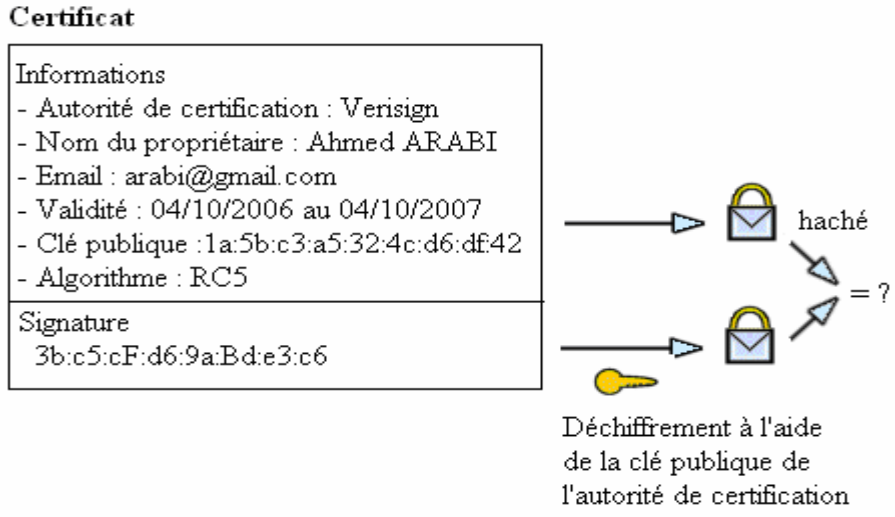
- Le nom de l'autorité de certification
- Le nom du propriétaire du certificat
- La date de validité du certificat
- L'algorithme de chiffrement utilisé
- La clé publique du propriétaire

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces

informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification.



Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire. Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats.



viii. SSL

SSL (en anglais Secure Sockets Layers, que l'on pourrait traduire par couche de sockets sécurisée) est un procédé de sécurisation des transactions effectuées via Internet. Il repose sur un procédé de cryptographie par clé publique afin de garantir la sécurité de la transmission de données sur Internet. Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP ou IMAP.

De cette manière, SSL est transparent pour l'utilisateur (entendez par là qu'il peut ignorer qu'il utilise SSL). Par exemple un utilisateur utilisant un navigateur Internet pour se connecter à un site de commerce électronique sécurisé par SSL enverra des données chiffrées sans avoir à s'en préoccuper.

La quasi intégralité des navigateurs supporte désormais le protocole SSL. Netscape Navigator affiche par exemple un cadenas verrouillé pour indiquer la connexion à un site sécurisé par SSL et un cadenas ouvert dans le cas contraire, tandis que Microsoft Internet Explorer affiche un cadenas uniquement lors de la connexion à un site sécurisé par SSL.

Un serveur sécurisé par SSL possède une URL commençant par https://, où le "s" signifie bien évidemment secured (sécurisé).

Fonctionnement de SSL 2.0

La sécurisation des transactions par SSL 2.0 est basée sur un échange de clés entre client et serveur. La transaction sécurisée par SSL se fait selon le schéma suivant:

- Dans un premier temps, le client, se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier. Le client envoie également la liste des cryptosystèmes qu'il supporte, triée par ordre décroissant de la longueur des clés.
- Le serveur a réception de la requête envoie un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA), ainsi que le nom du cryptosystème le plus haut dans la liste avec lequel il est compatible (la longueur de la clé de chiffrement - 40 bits ou 128 bits - sera celle du cryptosystème commun ayant la plus grande taille de clé).
- Le client vérifie la validité du certificat (donc l'authenticité du marchand), puis crée une clé secrète aléatoire (plus exactement un bloc prétendument aléatoire), chiffre cette clé à l'aide de la clé publique du serveur, puis lui envoie le résultat (la clé de session).
- Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée. Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs. Le reste des transactions peut se faire à l'aide de clé de session, garantissant l'intégrité et la confidentialité des données échangées.

Remarque : la notion de clé de session est un compromis entre le chiffrement symétrique et asymétrique permettant de combiner les deux techniques.
Le principe de la clé de session est simple : il consiste à générer aléatoirement une clé de session de taille raisonnable, et de chiffrer celle-ci à l'aide d'un algorithme de chiffrement à clé publique (plus exactement à l'aide de la clé publique du destinataire).
Le destinataire est en mesure de déchiffrer la clé de session à l'aide de sa clé privée. Ainsi, expéditeur et destinataires sont en possession d'une clé commune dont ils sont seuls connaisseurs. Il leur est alors possible de s'envoyer des documents chiffrés à l'aide d'un algorithme de chiffrement symétrique.

2. Protection contre les intrusions réseau

a. Pare-feu (FireWall)

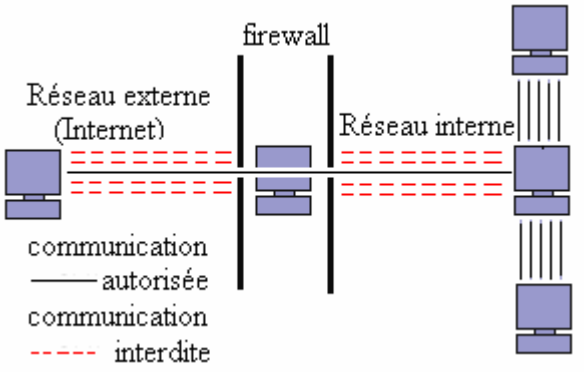
Introduction

Chaque ordinateur connecté sur Internet (ou sur n'importe quel réseau) est susceptible d'être victime d'intrusion pouvant compromettre l'intégrité du système ou des données. Les pirates informatiques s'introduisent dans les systèmes en recherchant des failles de sécurités dans les protocoles, les systèmes d'exploitations et les applications. Ils scrutent les réseaux dans

l'espoir de trouver un ordinateur mal protégé dans le quel, ils pourront s'introduire pour voler les données ou déposer des virus. Cette menace est encore plus importante si l'ordinateur est connecté en permanence à Internet.
Il est donc nécessaire, pour les entreprises, les établissements publics et les particuliers connectées à Internet avec une connexion de type réseau local, câble ou modem ADSL, de se protéger des intrusions en installant un système pare-feu.

Qu'est-ce qu'un pare-feu ?
Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment Internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une **passerelle filtrante** comportant au minimum les interfaces réseau suivants :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.



Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le traffic ;
- Le système soit sécurisé ;
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Le fonctionnement d'un système firewall
Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow ou accept) ;
- De bloquer la connexion (deny) ;
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en oeuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- soit d'autoriser uniquement les communications ayant été explicitement autorisées :
- soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

Le filtrage de paquets

Un système pare-feu fonctionnant sur le principe du filtrage de paquets analyse les en-têtes des paquets (aussi appelés datagrammes) échangés entre deux machines. En effet les machines d'un réseau relié à Internet sont repérées l'adresse IP.

Ainsi, lorsqu'une machine de l'extérieur se connecte à une machine du réseau local, et vice-versa, les paquets de données passant par le firewall contiennent les en-têtes suivants, qui sont analysés par le firewall:

- L'adresse IP de la machine émettrice
- L'adresse IP de la machine réceptrice
- Le type de paquet (TCP, UDP, ...)
- Le numéro de port (rappel: un port est un numéro associé à un service ou une application réseau)

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé. Certains ports sont associés à des service courants (les ports 25 et 110 sont généralement associés au courrier électronique, et le port 80 au Web) et ne sont généralement pas bloqués. Toutefois, il est nécessaire de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue).

Le tableau ci-dessous donne des exemples de règles de pare-feu :

Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

Un des ports les plus critiques est le port 23 car il correspond à l'utilitaire Telnet qui permet d'émuler un accès par terminal à une machine distante de manière à pouvoir exécuter des commandes saisies au clavier à distance...

Le filtrage applicatif

Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une connaissance de l'application, et notamment de la manière de laquelle elle structure les données échangées.

Un firewall effectuant un filtrage applicatif est appelé passerelle applicative car il permet de relayer des informations entre deux réseaux en effectuant un filtrage fin au niveau du contenu des paquets échangés.

Les limites des firewalls

Le fait d'installer un firewall n'est bien évidemment pas signe de sécurité absolue.

Les firewalls ne protègent en effet que des communications passant à travers eux. Ainsi, les accès au réseau extérieur non réalisés au travers du firewall sont autant de failles de sécurité. C'est par exemple le cas des connexions effectuées à l'aide d'un modem. D'autre part, le fait d'introduire des supports de stockage provenant de l'extérieur sur des machines internes au réseau peut être fort préjudiciable pour la sécurité de ce dernier.

La mise en place d'un firewall doit donc se faire en accord avec une véritable politique de sécurité. D'autre part la mise en place d'un système pare-feu n'exempt pas de se tenir au courant des failles de sécurité et d'essayer de les minimiser...

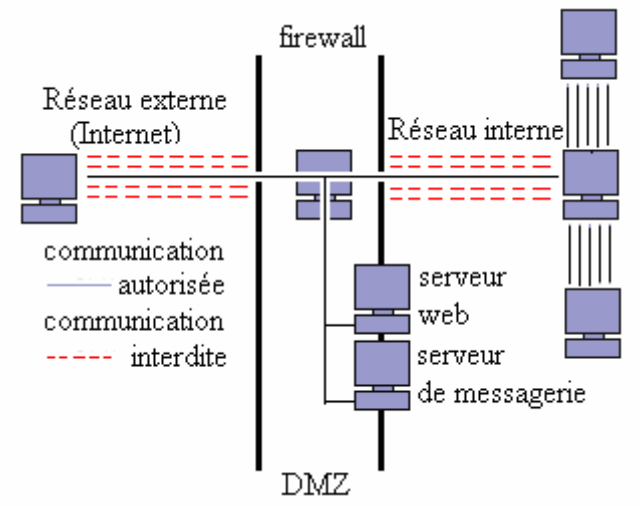
DMZ

Notion de cloisonnement

Les systèmes firewall permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feux permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « **cloisonnement des réseaux** » (le terme isolation est parfois également utilisé).

Architecture DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « **zone démilitarisé** » (notée **DMZ** pour DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public.



La politique de sécurité mise en oeuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé ;
- Trafic du réseau externe vers le réseau interne interdit ;
- Trafic du réseau interne vers la DMZ autorisé ;
- Trafic du réseau interne vers le réseau externe autorisé ;
- Trafic de la DMZ vers le réseau interne interdit ;
- Trafic de la DMZ vers le réseau externe refusé.

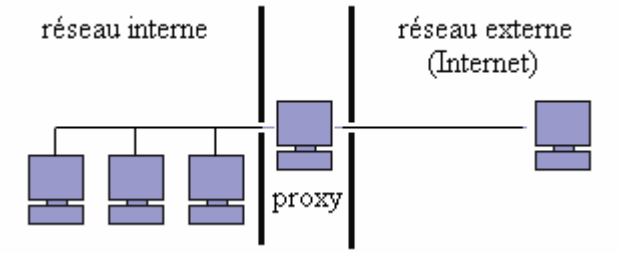
La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.
Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

b. Proxy

Introduction

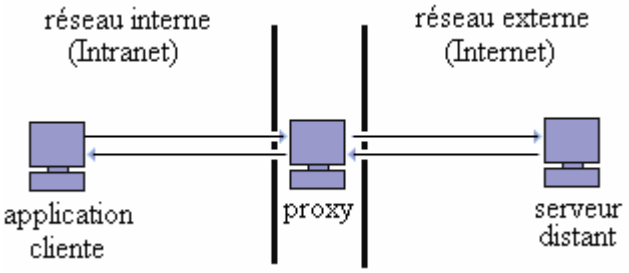
Un serveur proxy (traduction française de proxy server, appelé aussi serveur mandataire) est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et Internet.

La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...).



Le principe de fonctionnement d'un proxy

Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.



Les fonctionnalités d'un serveur proxy

Désormais, avec l'utilisation de TCP/IP au sein des réseaux locaux, le rôle de relais du serveur proxy est directement assuré par les passerelles et les routeurs. Pour autant, les serveurs proxy sont toujours d'actualité grâce à un certain nombre d'autres fonctionnalités.

La fonction de cache

La plupart des proxys assurent ainsi une fonction de **cache** (en anglais caching), c'est-à-dire la capacité à garder en mémoire (en "cache") les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les leur fournir le plus rapidement possible. En effet, en informatique, le terme de "cache" désigne un espace de stockage temporaire de données (le terme de "tampon" est également parfois utilisé).

Un serveur proxy ayant la possibilité de cacher (néologisme signifiant "mettre en mémoire cache") les informations est généralement appelé "serveur **proxy-cache**".

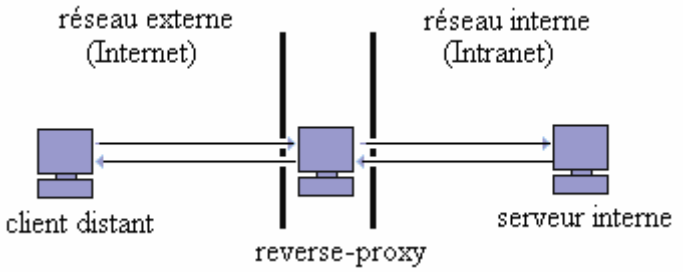
Cette fonctionnalité implémentée dans certains serveurs proxy permet d'une part de réduire l'utilisation de la bande passante vers Internet ainsi que de réduire le temps d'accès aux documents pour les utilisateurs.

Toutefois, pour mener à bien cette mission, il est nécessaire que le proxy compare régulièrement les données qu'il stocke en mémoire cache avec les données distantes afin de s'assurer que les données en cache sont toujours valides.

Le filtrage
D'autre part, grâce à l'utilisation d'un proxy, il est possible d'assurer un suivi des connexions (en anglais logging ou tracking) via la constitution de journaux d'activité (logs) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet.
Il est ainsi possible de filtrer les connexions à Internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs. Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de liste blanche, lorsqu'il s'agit d'une liste de sites interdits on parle de liste noire. Enfin l'analyse des réponses des serveurs conformément à une liste de critères (mots-clés, ...) est appelé filtrage de contenu.

L'authentification
Dans la mesure où le proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour authentifier les utilisateurs, c'est-à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple. Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistrer dans les fichiers journaux des accès identifiés.

Reverse-proxy
On appelle reverse-proxy (en français le terme de relais inverse est parfois employé) un serveur proxy-cache "monté à l'envers", c'est-à-dire un serveur proxy permettant non pas aux utilisateurs d'accéder au réseau Internet, mais aux utilisateurs d'Internet d'accéder indirectement à certains serveurs internes.

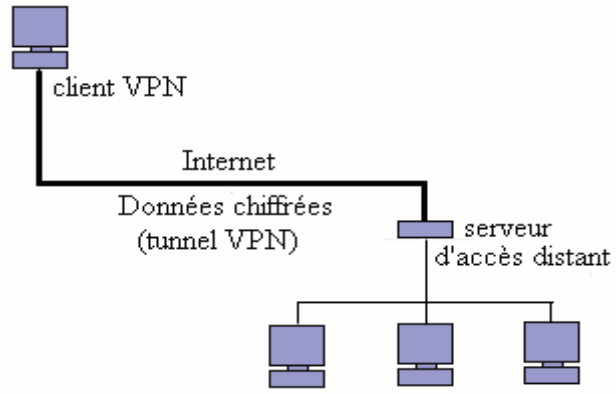


Le reverse-proxy sert ainsi de relais pour les utilisateurs d'Internet souhaitant accéder à un site web interne en lui transmettant indirectement les requêtes. Grâce au reverse-proxy, le serveur web est protégé des attaques directes de l'extérieur, ce qui renforce la sécurité du réseau interne. D'autre part, la fonction de cache du reverse-proxy peut permettre de soulager la charge du serveur pour lequel il est prévu, c'est la raison pour laquelle un tel serveur est parfois appelé "accélérateur" (server accelerator).
Enfin, grâce à des algorithmes perfectionnés, le reverse-proxy peut servir à répartir la charge en redirigeant les requêtes vers différents serveurs équivalents; on parle alors de "répartition de charge", ou en anglais "load balancing".

c. VPN
Le concept de VPN
Les réseaux locaux d'entreprise sont des réseaux internes à une organisation, c'est-à-dire que les liaisons entre machines appartiennent à l'organisation. Ces réseaux sont de plus en plus souvent reliés à Internet par l'intermédiaire d'équipements d'interconnexion. Il arrive ainsi souvent que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même des personnels géographiquement éloignés via Internet.

Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.
La première solution pour répondre à ce besoin de communication sécurisé consiste à relier les réseaux distants à l'aide de liaisons spécialisées. Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission.
Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole d'"encapsulation" (en anglais tunneling) c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de **réseau privé virtuel** (**VPN**, acronyme de Virtual Private Network) pour désigner le réseau ainsi artificiellement créé.
Ce réseau est dit virtuel car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent "voir" les données.
Le système de VPN permet donc d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en oeuvre des équipements terminaux. En contrepartie il ne permet pas d'assurer une qualité de service comparable à une ligne louée dans la mesure où le réseau physique est public et donc non garanti.

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



Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de l'organisation.
De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur ...

Les protocoles de tunnelisation
Les principaux protocoles de tunneling sont les suivants :

- PPTP (Point-to-Point Tunneling Protocol) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète
- L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- IPSec est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

IV. Audit de Vulnérabilités

1. Introduction

L'audit de vulnérabilité permet d'adopter une approche automatisée et exhaustive des tests de sécurité. En aucun cas il remplace le test d'intrusion qui lui intervient en amont de tout projet sécurité car il permet de déceler des faiblesses sur les architectures. De plus, le test d'intrusion permet également de sensibiliser la direction aux problématiques sécurité et aide dans bien des cas à obtenir des budgets pour la sécurité. L'audit de vulnérabilités possède une approche plus régulière que le test d'intrusion, il doit permettre de mesure le niveau de sécurité et de contrôler l'imperméabilité du réseau. Dans le cas ou les résultats ne sont pas satisfaisants, l'audit de vulnérabilités doit conduire à un processus de remediation des vulnérabilités découvertes. En entreprise, on s'attache aujourd'hui davantage à la gestion des vulnérabilités qui contient la phase d'audit mais aussi tous les processus permettant la distribution des informations pour la remediation et le contrôle récurent des installations.

2. Le concept de l'audit de vulnérabilités

Aujourd'hui, votre réseau informatique possède un niveau de sécurité élevé. Vos serveurs et machines sont à jour, aucune vulnérabilité connue touche vos systèmes, mais demain ? En effet, tous les jours de nouvelles vulnérabilités sont découvertes. Ces failles peuvent toucher les systèmes d'exploitation ou services que vous possédez au sein de votre infrastructure. Comment être alerté au plus tôt de la présence d'une vulnérabilité qui affecte vos équipements ? Cette problématique trouve sa réponse dans les audits de vulnérabilités récurrents et l'adoption d'une démarche proactive.
Pourquoi attendre que votre service de veille vous avertisse de la sortie d'une nouvelle faille alors que vous pourriez, a peine quelques heures après sa découverte, en tester la présence réelle sur vos machines et détecter instantanément si vous êtes vulnérable ou non ?
De nombreuses solutions d'audits de vulnérabilités automatisés existent. Les technologies ont beaucoup évoluée et il est désormais possible de détecter avec une grande précision les vulnérabilités connues. L'audit automatisé et récurrent permet d'adopter une démarche proactive dans la gestion des vulnérabilités qui peuvent toucher vos réseaux.
Pour garantir dans le temps un niveau de sécurité élevé, il est impératif de tester de manière récurrente et rapprochée l'ensemble des éléments critiques qui constituent votre infrastructure.

Une approche proactive
Une démarche proactive dans la gestion des vulnérabilités est la clé du maintien d'un niveau de sécurité élevé sur vos systèmes. Il faut aller au devant des vulnérabilités et les traiter le plus rapidement possible avant un incident.

Un audit de vulnérabilités se déroule généralement en quatre phases. Ces phases sont les piliers de la démarche proactive de gestion de vulnérabilités.

Phase de découverte
La première phase d'un audit de vulnérabilités est la découverte des machines à auditer. Il faut connaître avec précision son périmètre réseau aussi bien interne que externe. Certaines solutions offrent des fonctionnalités de mapping qui permet d'effectuer un inventaire du parc interne ou externe et de choisir les machines à tester. Évidemment les machines dites "sensibles" sont les premières à auditer mais il ne faut pas néanmoins négliger les autre y compris les stations de travail qui, nous l'avons vu avec l'arriver de vers comme "sasser" ou "blaster", sont des cibles de choix pour les développeurs de virus.

Phase de détection
La phase de détection ou "Assessment" correspond à la détection des vulnérabilités présentes sur les machines testées. Cette phase doit être opérée de manière récurrente et automatisée. A partir de la base de connaissance de la solution d'audits, celle-ci va déterminer les vulnérabilités présentes sur une ou plusieurs machines ou éléments actifs. En fonction de la solution utilisée, cette phase peut être plus ou moins intrusive. Certains éditeurs de solutions d'audit de vulnérabilités adoptent une politique "non intrusive" afin de pouvoir tester sans risques des serveurs en production.

Phase d'analyse des résultats
Cette phase correspond à l'exploitation des résultats de la phase de test. La solution d'audits de vulnérabilités doit être à même de fournir un reporting précis pour les équipes techniques, détaillant les problèmes rencontrés, l'impact sur les machines et les solutions pour corriger les failles. Certains solutions offrent également des rapport dits "Executive" qui n'étant pas techniques, s'adressent plus à une direction informatique faisant un état des lieux du niveau de sécurité global du système informatique et fournis également des rapports d'analyse de tendance sur une période donnée. Cela permet en outre aux directions de visualiser l'efficacité de leurs équipes sécurité et de pouvoir visualiser leurs retours sur investissements dans le domaine de la protection de l'infrastructure informatique de l'entreprise.

Phase de remediation
Cette dernière phase a pour but de gérer au mieux les interventions qui font suite aux découvertes. Certaines solutions d'audits de vulnérabilités fournissent une plateforme d'attribution de ticket lors de la découverte d'une vulnérabilité. Le ticket adressé à un technicien lui permet de mettre en place une action curative et de tracer les événements de remediation. Le processus de remediation doit être l'aboutissement d'un audit de vulnérabilités.

3. COBIT

Le référentiel COBIT (Control Objectives for Information and related Technologies, traduisez contrôler les objectifs des technologies de l'information) est une méthode de maîtrise des systèmes d'information et d'audit de systèmes d'information, éditée par l'Information System Audit & Control Association (ISACA) en 1996. C'est un cadre de contrôle qui vise à aider le management à gérer les risques (sécurité, fiabilité, conformité) et les investissements.
Il y a un certain nombre d'outils qui ont été mis en place afin de coller aux besoins des entreprises selon leur importance et la complexité de leurs systèmes d'informations.
L'objectif du COBIT était de faire le lien entre les risques métiers, les besoins de contrôle et les questions techniques en se basant sur les meilleures pratiques en audit informatique et systèmes d'informations.

Les outils mis à notre disposition :

COBIT QuickStart : propose une première approche aux nombreuses PME et autres entités pour lesquelles les technologies d'information ne sont ni un enjeu stratégique ni un élément clé de leur survie ; pour d'autres entreprises il constitue un point de départ dans leur évolution vers un niveau de contrôle et de gouvernance des technologies d'information adapté à leurs besoins.

COBIT ONLINE est un site web réalisé par l'IT Governance Institute accessible par abonnement à l'adresse : www.isaca.org/cobitonline Il offre diverses fonctionnalités comme la possibilité de pouvoir consulter et télécharger le contenu de COBIT en ligne, de réaliser des analyses comparatives (benchmark) et d'échanger avec d'autres utilisateurs (forum).

COBIT Advisor : ce logiciel facilite la conduite d'un audit informatique et la génération de rapports et de représentations graphiques des résultats.

V. La disponibilité des données

1. Sauvegarde et archivage

a. Introduction

Il paraîtrait presque normal de confondre sauvegarde et archivage. Après tout, il s'agit dans les deux cas de stocker des données sur un support de masse afin de les conserver. Ce serait cependant une erreur ! Et comprendre la différence qui existe entre une sauvegarde et une archive permet de mieux appréhender le cycle de vie de la donnée dans l'entreprise et le choix des solutions techniques.

Pour cela, un retour historique s'impose. Les vétérans de l'informatique parlaient plus volontiers de stockage "chaud" ou "froid" plutôt que de sauvegarde ou d'archivage. Le stockage dit "chaud" était la donnée immédiatement accessible et facilement modifiable. A l'opposé, le stockage dit "froid" désignait la donnée archivée sur un support à très forte capacité de stockage, mais dont l'inconvénient était de ne pas permettre une récupération rapide et granulaire des informations. Ainsi, une fois les enregistrements "descendus" sur une bande magnétique, la récupération d'un fichier particulier situé en milieu de bande pouvait prendre plusieurs heures et n'était de ce fait utilisée qu'en dernier recours.

De cette distinction finalement technique découlent les notions de sauvegarde et d'archivage. Les données sauvegardées sont susceptibles d'être récupérées rapidement et peuvent être modifiées à volonté. Mais au delà d'un certain délai, ou lorsque la donnée a été "consommée" et traitée, elle est enregistrée sur une bande où elle ne sera plus modifiée (archivée, donc) afin d'être conservée en l'état.

En résumé: on n'accède quasiment jamais aux archives tandis que l'on passe son temps à modifier des sauvegardes, ne serait-ce que pour les mettre à jour !

b. Stratégies de sauvegarde

Un certain nombre de facteurs sont à prendre en compte lors de la planification de la solution : sauvegarde des éléments nécessaires seulement, planification soigneuse des sauvegardes et choix du type approprié de sauvegarde à exécuter.

Nécessité d'éviter les sauvegardes superflues
Lorsque vous concevez une stratégie de sauvegarde, vous pouvez être tenté d'exécuter une sauvegarde intégrale de chaque serveur de l'environnement. Gardez à l'esprit cependant que votre objectif est de restaurer correctement l'environnement après une panne ou une catastrophe. Votre stratégie de sauvegarde doit donc se concentrer sur les objectifs suivants :

- les données à restaurer doivent être aisément localisables ;
- la restauration doit s'avérer aussi rapide que possible.

Si vous sauvegardez tous les serveurs sans distinction, vous aurez un gros volume de données à restaurer. Bien que les produits de sauvegarde et de restauration permettent une restauration rapide des données, le temps d'arrêt peut s'allonger si vous devez tout restaurer à partir d'une bande. Ainsi, la plupart des produits de sauvegarde nécessitent l'exécution des étapes suivantes :

- réinstallation du système d'exploitation ;
- réinstallation du logiciel de sauvegarde ;
- restauration des données sauvegardées sur bande.

Plus vous sauvegardez de fichiers, plus la sauvegarde est longue, et surtout, plus la restauration des fichiers prend de temps. Après une catastrophe, le facteur temps est une donnée majeure. C'est pourquoi il importe que le processus de restauration soit aussi court que possible. En outre, les grosses sauvegardes effectuées de manière régulière ont un effet néfaste sur les performances du réseau à moins que vous ne mettiez en place un réseau de sauvegarde dédié.
Une fois que vous avez déterminé la stratégie de sauvegarde optimale pour votre environnement, il est indispensable d'effectuer une restauration-test sur la globalité du réseau test. Cet essai permet d'identifier les zones à problème et constitue une expérience utile en matière de restauration des systèmes dans l'environnement sans subir la pression de la remise en ligne du système de production.

Choix du moment approprié pour les sauvegardes
Chaque type d'environnement présente différentes opportunités pour effectuer une sauvegarde efficace en interrompant le moins possible les utilisateurs. Ainsi, la sauvegarde d'un environnement de commerce électronique n'a pas la même implication que la sauvegarde de l'infrastructure d'un réseau local d'entreprise. Sur un réseau LAN d'entreprise, l'utilisation est moindre en dehors des principales heures de travail. Dans un environnement de commerce électronique, l'utilisation augmente généralement en début de soirée et peut se poursuivre ainsi jusqu'aux premières heures de la matinée, particulièrement si la base de clients couvre plusieurs fuseaux horaires. C'est pour cette raison qu'il n'est pas possible de déterminer l'heure idéale de sauvegarde de votre environnement.

Choix du support de stockage le mieux adapté
Après avoir déterminé le type de sauvegarde à effectuer et le moment approprié pour cette opération, vous devez également étudier les types de supports de stockage disponibles et sélectionner le support le mieux adapté.
Lorsque vous choisissez un support de stockage, tenez compte des points suivants :

- quantité de données à sauvegarder ;
- type de données à sauvegarder ;
- distance entre les systèmes à sauvegarder et le périphérique de stockage ;
- budget de votre entreprise ;
- … .

Le tableau suivant récapitule les avantages et inconvénients des types de supports de sauvegarde les plus courants.

Type de support de sauvegarde	Avantages	Inconvénients
Bande	Assure une sauvegarde rapide et une longue conservation des données. Offre une capacité de stockage étendue. Plus économique que les disques magnétiques et magnéto-optiques.	S'use plus rapidement et se révèle plus sujet aux erreurs que les disques magnétiques et magnéto-optiques. Difficile à configurer et à maintenir, particulièrement dans une configuration de réseau de stockage (SAN). Requiert un nettoyage périodique des périphériques.
Disque magnétique	Facile à configurer et à entretenir. Utilisable pour les données intermédiaires.	Support le plus onéreux pour un stockage initial.
Disque magnéto-optique	Affiche la plus longue durée de vie sans dégradation du support.	Ralentit la sauvegarde et la restauration des données. Limite le choix du matériel.

c. Mode de sauvegarde

Le mode de sauvegarde détermine la façon dont la sauvegarde a lieu en fonction des données à sauvegarder. Il existe deux méthodes pour sauvegarder les données :

- Sauvegardes en ligne : les sauvegardes s'effectuent pendant que les données restent accessibles à tous les utilisateurs.
- Sauvegardes hors ligne : les sauvegardes concernent les données qui sont d'abord mises hors de portée des utilisateurs.

Sauvegardes en ligne

Les sauvegardes en ligne ont lieu pendant que le système est en ligne. C'est la stratégie de l'interruption la plus courte. Ce type de sauvegarde est généralement utilisé pour les applications devant être disponibles 24 heures/24, telles que Microsoft Exchange Server et Microsoft SQL Server, les deux prenant en charge les sauvegardes en ligne.

Avantages

Parmi les avantages des sauvegardes en ligne, on retient :

- Pas d'interruption de service : Les applications et les données restent entièrement accessibles aux utilisateurs pendant le processus de sauvegarde.
- La sauvegarde hors des heures de travail n'est plus nécessaire : Les sauvegardes en ligne peuvent être programmées pendant les heures normales de bureau.
- Sauvegarde partielle ou totale : Les sauvegardes peuvent être partielles ou totales.

Inconvénients

Parmi les inconvénients des sauvegardes en ligne, on retient :

- Performances du serveur : Au cours du processus de sauvegarde, il est possible que les performances des serveurs de production se dégradent.
- Fichiers ouverts
- Si certaines applications sont actives pendant le processus de sauvegarde, il est possible que les fichiers de données ouverts ne soient pas sauvegardés.

Sauvegardes hors ligne

Les sauvegardes hors ligne sont effectuées en mettant hors ligne le système et les services. Vous pouvez les utiliser si vous avez besoin d'un instantané du système ou si l'application ne prend pas en charge les sauvegardes en ligne.

Avantages

Parmi les avantages des sauvegardes hors ligne, on retient :

- Sauvegarde partielle ou totale : Avec les sauvegardes hors ligne, vous pouvez choisir entre une sauvegarde partielle ou totale.
- Performances : Les sauvegardes hors ligne offrent de meilleures performances de sauvegarde car le serveur peut être dédié à la tâche de sauvegarde.
- Sauvegarde de tous les fichiers : Toutes les données sont sauvegardées dans la mesure où aucune application n'est en cours d'exécution et donc qu'aucun fichier n'est ouvert pendant le processus de sauvegarde.

Inconvénient

- Interruption du service : L'inconvénient des sauvegardes hors ligne est que les données ne sont pas accessibles à l'utilisateur pendant l'exécution du processus de sauvegarde.

d. Types de sauvegarde

Les différents types de sauvegarde peuvent être utilisés pour des sauvegardes hors ligne ou en ligne. Ce sont les exigences d'accord sur le niveau de sauvegarde de l'environnement, de fenêtre de sauvegarde et de durée de restauration qui déterminent la méthode ou la combinaison de méthodes optimales pour cet environnement.

Sauvegardes intégrales

L'objectif de la sauvegarde intégrale (parfois sauvegarde complète ou en anglais full backup) est de réaliser une copie conforme des données à sauvegarder sur un support séparé.

Vous pouvez utiliser une bande de sauvegarde intégrale à jour pour restaurer entièrement le serveur à un instant t.

Sauvegardes incrémentielles

Une sauvegarde incrémentielle (en anglais incremental backup) capture la moindre donnée qui a été modifiée depuis la dernière sauvegarde intégrale ou incrémentielle. Vous devez utiliser une bande de sauvegarde intégrale (son ancienneté importe peu) et tous les jeux suivants de sauvegardes incrémentielles pour restaurer un serveur.

Avantages

Parmi les avantages des sauvegardes incrémentielles, on retient :

- Optimisation du temps : Le processus de sauvegarde prend moins de temps dans la mesure où ne sont copiées sur la bande que les données modifiées ou créées depuis la dernière sauvegarde incrémentielle ou intégrale.
- Optimisation du support de sauvegarde : La sauvegarde incrémentielle utilise moins de bande puisque ne sont copiées sur la bande que les données modifiées ou créées depuis la dernière sauvegarde incrémentielle ou intégrale.

Inconvénients

Parmi les inconvénients des sauvegardes incrémentielles, on retient :

- Complexité de la restauration complète : La restauration d'un système complet doit passer par la restauration d'un ensemble incrémentiel de plusieurs bandes.
- Restaurations partielles chronophages : Une restauration partielle implique de rechercher sur plusieurs bandes les données requises.

Sauvegardes différentielles

Une sauvegarde différentielle (en anglais differential backup) capture les données qui ont été modifiées depuis la dernière sauvegarde intégrale. Pour effectuer une restauration du système, vous aurez besoin de la bande de sauvegarde intégrale et de la bande de sauvegarde différentielle la plus récente.

Avantage

- Restauration rapide : L'avantage que présentent les sauvegardes différentielles tient dans le fait que leurs restaurations sont plus rapides que celles des sauvegardes incrémentielles car elles impliquent moins de bandes. Une restauration complète nécessite deux jeux de bandes au plus : la bande de la dernière sauvegarde intégrale et celle la dernière sauvegarde différentielle.

Inconvénients

Parmi les inconvénients des sauvegardes différentielles, on retient :

- Des sauvegardes plus volumineuses et plus longues : Les sauvegardes différentielles demandent plus d'espace sur la bande et plus de temps que les sauvegardes incrémentielles car plus la période qui vous sépare de la dernière sauvegarde intégrale est longue, plus il y aura de données à copier sur la bande différentielle.
- Augmentation de la durée de la sauvegarde : Le volume de données à sauvegarder augmente chaque jour qui suit une sauvegarde intégrale.

e. Topologies de sauvegarde

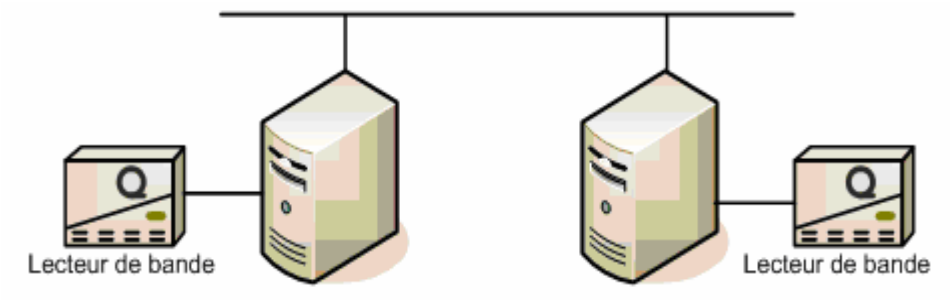
À l'origine, le seul type de technologie de stockage qui nécessitait une sauvegarde impliquait l'utilisation de disques durs connectés directement aux adaptateurs de stockage sur les serveurs. Aujourd'hui, ce type de stockage est connu sous le nom de stockage direct connecté (DAS). Le paysage de la sauvegarde et de la restauration a nettement évolué avec le développement de technologies telles que les SAN et NAS. Les environnements SAN en particulier fournissent un moyen intéressant d'optimiser et de simplifier le processus de sauvegarde et de restauration.

Les topologies de sauvegarde et de restauration peuvent être classées en fonction de la technologie de stockage (DAS, NAS ou SAN) à sauvegarder. Les topologies couvrant chaque type de stockage sont respectivement la sauvegarde par serveur local, les sauvegardes NAS liées à un réseau LAN et les systèmes sur SAN.

Sauvegarde et restauration par serveur local

Dans le cadre d'une configuration de sauvegarde par serveur local, chaque serveur se connecte à son propre dispositif de sauvegarde, via généralement un bus SCSI. La bande passante du réseau local (LAN) n'est pas utilisée ici, mais vous devez gérer manuellement le support de stockage sur le serveur local.

La figure suivant présente un mécanisme type de sauvegarde et restauration par serveur local.



Avantages

Parmi les avantages de la sauvegarde et de la restauration par serveur local, on retient :

- Ressources réseau non consommées : Les configurations de sauvegarde et de restauration par serveur local n'utilisent pas la bande passante du réseau car les serveurs sont généralement connectés aux dispositifs à bandes par une interface SCSI.
- Une sauvegarde et une restauration plus rapides : Ces sauvegardes peuvent être plus rapides que toute autre configuration de sauvegarde dans la mesure où les données n'ont pas à transiter sur le réseau.

Inconvénients

Parmi les inconvénients de la sauvegarde et de la restauration par serveur local, on retient :

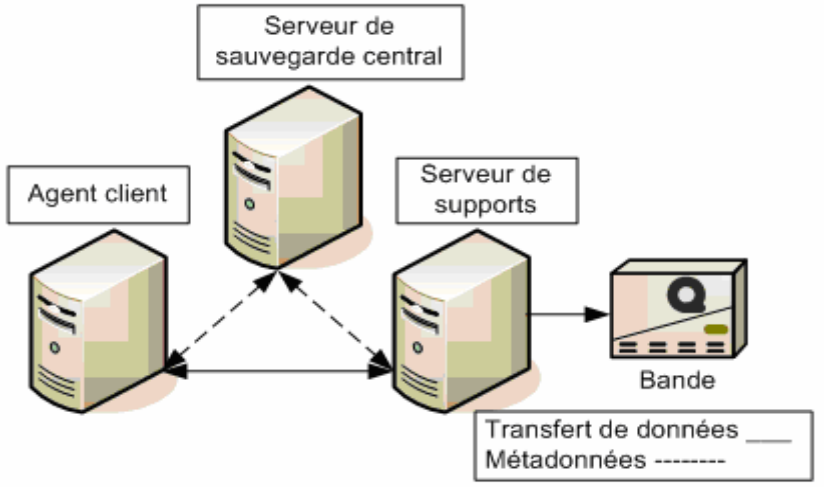
- Capacité limitée de gestion centralisée et d'évolution possible : La configuration de sauvegarde et de restauration par serveur local n'offre pas de possibilités d'évolution ni de gestion centralisée car les supports de stockage doivent être gérés localement, au niveau de chaque serveur.
- Des coûts plus élevés en termes de logiciels de sauvegarde et de bandes : Cette configuration peut augmenter considérablement les coûts en licences de logiciel de sauvegarde et en périphériques à bandes dans la mesure où vous devez configurer une sauvegarde par serveur et les gérer individuellement.

Sauvegarde et restauration par réseau LAN

Les installations de sauvegarde par réseau LAN constituent une solution courante dans les entreprises et sont utilisées depuis un certain temps déjà. Un logiciel de sauvegarde LAN de l'entreprise fait appel à une architecture multi-couche selon laquelle certains serveurs de sauvegarde démarrent leur activité et collectent des méta-données (également appelées données de contrôle) sur les données sauvegardées pendant que d'autres serveurs (appelés serveurs de support) gèrent effectivement les données transférées sur les lecteurs de bandes.
Les technologies de sauvegarde LAN de l'entreprise sont généralement composées de trois éléments :

- Un serveur central de sauvegarde : Ce serveur héberge le moteur de sauvegarde qui contrôle l'environnement de sauvegarde.
- Un serveur de support : Ce serveur gère le mouvement des données et contrôle les ressources des supports.
- Des agents clients : Il s'agit des agents spécifiques d'applications, tels que pour les données Exchange, les données SQL Server et les données du système de fichiers.

La figure qui suit illustre un système de sauvegarde et de restauration logique LAN :



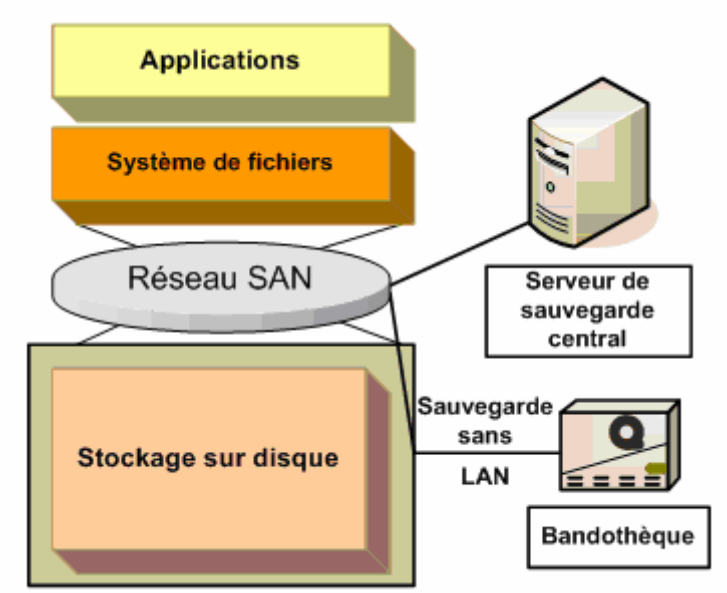
Avantages
Parmi les avantages de la sauvegarde et de la restauration par réseau LAN, on retient :

- Les lecteurs de bandes n'ont plus besoin d'être connectés directement aux serveurs pour la sauvegarde.
- L'application de sauvegarde s'exécute sur des serveurs de sauvegarde dédiés.
- Les agents clients dirigent les données du LAN vers un serveur de sauvegarde.
- Meilleures possibilités d'évolution et partage des dispositifs à bandes.

Inconvénients
Parmi les inconvénients de la sauvegarde et de la restauration par réseau LAN, on retient :

- Les lots volumineux de données peuvent entraîner une dégradation des performances des serveurs et du réseau.
- Le trafic supplémentaire généré par la sauvegarde consomme la bande passante du réseau.
- La planification des sauvegardes et des restaurations peut devenir critique.

Sauvegarde et restauration sur SAN
La possibilité d'intégrer des sous-systèmes d'espace disque à la sauvegarde et à la restauration vous offre un certain nombre d'options pour déployer les solutions de protection des données dans des environnements SAN. Les technologies sous-jacentes SAN fournissent plusieurs alternatives de sauvegarde et de restauration des données résidant sur un stockage SAN.
La figure ci dessous illustre un scénario de sauvegarde sur SAN



Avantages
Parmi les avantages de la sauvegarde et de la restauration sur SAN, on retient :

- Une charge réduite du serveur : Le chemin entre le dispositif de stockage et celui de sauvegarde n'implique pas la présence d'un serveur, ce qui signifie que la charge du serveur est réduite.
- Une charge réduite du réseau : Les sauvegardes peuvent s'effectuer sans avoir à faire transiter les données sur le réseau LAN.
- Une solution de stockage optimisée : Les réseaux SAN sont conçus pour optimiser l'efficacité des transferts de données et permettre ainsi d'accélérer les processus de sauvegarde et de restauration.

Inconvénients
Parmi les inconvénients de la sauvegarde et de la restauration sur SAN, on retient :

- Les dépenses : Les sauvegardes sur SAN nécessitent un réseau SAN, dont la conception et le déploiement s'avèrent coûteux.
- La compatibilité des dispositifs : Les équipements de sauvegarde et de restauration doivent être compatibles SAN.

2. Plans de relève
a. Plan de relève informatique
Les plans de relève informatiques sont les précurseurs des plans de relève corporatifs.
Longtemps considérée comme une fonction essentielle des entreprises, celles ci se rendent compte aujourd'hui que l'informatique est rarement leur raison d'être. C'est ce qui explique que plusieurs grandes entreprises se tournent vers la sous-traitance ou l'impartition.
Plusieurs stratégies s'offrent à nous et des choix éclairés doivent être faits afin de maintenir les coûts de continuité à un niveau acceptable.
Le choix du site de relève (interne ou commercial) et du type de site désiré (équipé complètement, partiellement ou non équipé) influence grandement le coût de la relève.
L'avènement des liens de télécommunications à très haut débit, à coût modéré permet d'être beaucoup plus imaginatif qu'il y a 10 ans. La distance entre le site de production et de relève est de moins en moins un critère de sélection. Les données critiques peuvent maintenant être protégées jusqu'à la dernière transaction sur des distances impressionnantes.
La protection des données par de simples prises de copies, suivi d'une sortie manuelle dans une voûte devient presque désuète puisque souvent ils peuvent être pris à distance, offrant ainsi une protection instantanée. Notons que la possibilité de prendre des copies à distance est disponible maintenant pour toutes les entreprises, grandes ou petites.
Plusieurs plans de relève ne comportent qu'une suite de procédures techniques destinées à relever l'environnement informatique. La portion administrative est souvent laissée de coté, à tors. Un processus clair et documenté d'évaluation des dommages et d'activation du plan permet d'accélérer la prise de décision, donc la mise en place de l'environnement de relève.
Un plan devrait comporter un processus d'évaluation, d'activation et d'escalade, une procédure de mise en place au site de relève, les procédures de remontée des environnements de base et des applications, différentes listes (personnel, équipement, liens, fournisseurs, documentation, etc…), et une section décrivant le manuel, sa structure et son processus de maintenance

b. Plan de relève corporatif
Un plan de relève corporatif permet de protéger une entreprise contre tout événement qui pourrait engendrer un arrêt de ses opérations.
Quand on pense « arrêt des opérations » on a tendance à penser aux sinistres majeurs tel feu, inondation et tremblement de terre. Un bon plan de relève doit adresser ces alternatives, mais doit principalement être ciblé vers les risques potentiels.
Pour se protéger contre ces risques potentiels, des stratégies de relève ou plans d'actions seront élaborés. Ces stratégies identifieront un ou des sites de production alternatifs, les composantes requises ainsi que des processus de remplacement de ces composantes à court, moyen ou long terme et les ressources humaines et informationnelles requises pour que l'entreprise puisse continuer d'opérer.
Des mesures de protection seront mises en place afin de protéger les données informatiques ou opérationnelles contre un bris ou un sinistre.
La structure du plan de relève corporatif est similaire au plan de relève informatique. La différence entre ces 2 plans provient du fait qu'un plan de relève informatique est un sous-ensemble du plan de relève corporatif.

Le plan de relève corporatif sera constitué des processus et procédures suivants :

- un processus d'évaluation du sinistre ;
- une procédure d'activation du plan
- une procédure d'appel et d'escalade
- une procédure d'activation et de mise en place du ou des sites alternatifs ;
- une procédure de recouvrement des environnements informatiques et bureautiques affectés
- une procédure pour rediriger les liens de télécommunications voix et données au(x) site(s) alternatif(s)
- les procédures de récupération des données informatiques et opérationnelles
- les procédures administratives
- un processus de maintenance afin d'éviter la désuétude du plan

Les listes utiles (ressources humaines, ressources physiques, liens de télécommunications, équipements requis, papeterie et formulaires, données vitales).
Afin de gérer toutes ces informations, il existe des outils spécialisés qui faciliteront le développement et le maintien des plans de relève. Certains outils sont valables alors que d'autres n'ont que peu de valeur ajoutée. L'utilisation d'un bon traitement de texte, jumelé à une structure de plan bien définie peuvent très bien faire l'affaire.
L'utilisation d'experts en continuité des affaires permet d'accélérer les étapes de développement d'un plan de relève et ainsi donc, de réduire les coûts de développement et d'accélérer la protection de l'entreprise.

c. Continuité des affaires

Au Québec, l'intérêt des grandes entreprises pour les plans de relève s'est réveillé suite au feu de la Plaza Alexis Nihon, à la fin des années 1980, où étaient établis les locaux informatiques de chaîne alimentaire Steinberg. Cette firme, venait de compléter l'élaboration de son plan de relève informatique et de terminer un test dans son site de relève.
C'est à ce moment là que plusieurs dirigeants québécois ont réalisé leur niveau de dépendance envers leur centre informatique et qu'ils ont démarré l'élaboration des premiers plans de relève informatique.
Une fois ces plans réalisés, une autre question de posait : Mon application est maintenant protégée, mais qu'adviendrait-il si un sinistre affectait le client de cette application ? Et c'est en réponse à cette question que les plans de relève corporatifs sont apparus.
Depuis, plusieurs sociétés importantes se sont dotées de plans afin de répondre à un sinistre majeur. Mais, est-ce uniquement ce type d'évènement qui peut vous affecter ?
L'industrie de la relève tend de plus en plus à utiliser le concept de « Continuité des affaires ».
Par ce concept, nous analysons tout type d'évènements qui pourraient entraver la bonne marche d'une entreprise, donc la continuité de ses affaires. L'utilisation d'une telle étude, de concert avec une analyse d'impacts commerciale, nous permet de produire un plan d'action afin de mettre en place des mesures préventives et correctrices qui sont adaptées aux besoins de l'entreprise.
Avec en main un programme de prévention adapté, un plan de relève adéquat pour pallier à tout type d'interruption de services, un plan de maintenance formel, des tests complets et fréquents et un programme de formation adéquat, vous pourrez dormir paisiblement sans vous demander si votre entreprise sera là demain, ou la semaine prochaine...

Etapes de la mise en place d'un plan de continuité

Pour qu'un plan de continuité soit réellement adapté aux exigences de l'entreprise, il doit reposer sur une analyse de risque et une analyse d'impact :

L'analyse de risque débute par une identification des menaces sur l'informatique. Les menaces peuvent être d'origine humaine (attaque délibérée ou maladresse) ou d'origine « naturelle »; elles peuvent être internes à l'entreprise ou externes. On déduit ensuite le risque qui découle des menaces identifiées; on mesure l'impact possible de ces risques. Enfin, on décide de mettre en œuvre des mesures d'atténuation des risques en se concentrant sur ceux qui ont un impact significatif. Par exemple, si le risque de panne d'un équipement risque de tout paralyser, on installe un équipement redondant. Les mesures d'atténuation de risque qui sont mises en œuvre diminuent le niveau de risque, mais elles ne l'annulent pas: il subsiste toujours un risque résiduel, qui sera couvert soit par le plan de continuité, soit par d'autres moyens (assurance, voire acceptation du risque)

L'analyse d'impact consiste à évaluer quel est l'impact d'un risque qui se matérialise et à déterminer à partir de quand cet impact est intolérable, généralement parce qu'il met en danger les processus essentiels (donc, la survie) de l'entreprise. L'analyse d'impact se fait sur base de désastres: on considère des désastres extrêmes, voire improbables (par exemple, la destruction totale du bâtiment) et on détermine les impacts financiers, humains, légaux, etc., pour des durées d'interruption de plus en plus longues jusqu'à ce qu'on atteigne l'impact maximal tolérable. Le résultat principal de l'analyse d'impact est donc une donnée temporelle: c'est la durée maximale admissible d'une interruption de chaque processus de l'entreprise. En tenant compte des ressources informatiques (réseaux, serveurs, PCs…) dont chaque processus dépend, on peut en déduire le temps maximal d'indisponibilité de chacune de ces ressources, en d'autres termes, le temps maximal après lequel une ressource informatique doit avoir été remise en fonction

Une analyse de risque réussie est le résultat d'une action collective impliquant tous les acteurs du système d'information : techniciens, utilisateurs et managers.

Choix de la stratégie de sécurisation

Il existe plusieurs méthodes pour assurer la continuité de service d'un système d'information. Certaines sont techniques (choix des outils, méthodes de protection d'accès et de sauvegarde des données), d'autres reposent sur le comportement individuel des utilisateurs (extinction des postes informatiques après usage, utilisation raisonnable des capacités de transfert d'informations, respect des mesures de sécurité), sur des règles et connaissances collectives (protection incendie, sécurité d'accès aux locaux, connaissance de l'organisation informatique interne de l'entreprise) et de plus en plus sur des conventions passées avec des prestataires (copie des programmes, mise à disposition de matériel de secours, assistance au dépannage).

Les méthodes se distinguent entre **préventives** (éviter la discontinuité) et **curatives** (rétablir la continuité après un sinistre). Les méthodes préventives sont souvent privilégiées, mais décrire les méthodes curatives est une nécessité car aucun système n'est fiable à 100 %.

Mesures préventives

La sauvegarde des données

La préservation des données passe par des copies de sauvegarde régulières. Il est important de ne pas stocker ces copies de sauvegarde à côté du matériel informatique, voire dans la même pièce car elles disparaîtraient en même temps que les données à sauvegarder en cas d'incendie, de dégât des eaux, de vol, etc. Lorsqu'il est probable que les sauvegardes disparaissent avec le matériel, le stockage des copies de sauvegarde peut alors être nécessaire dans un autre lieu différent et distant.

- **Les systèmes de secours**

Il s'agit de disposer d'un système informatique équivalent à celui pour lequel on veut limiter l'indisponibilité : ordinateurs, périphériques, systèmes d'exploitation, programmes particuliers, etc. Une des solutions consiste à créer et maintenir un **site de secours**, contenant un système en ordre de marche capable de prendre le relais du système défaillant. Selon que le système de secours sera implanté sur le site d'exploitation ou sur un lieu géographiquement différent, on parlera d'un secours in situ ou d'un secours déporté.
Pour répondre aux problématiques de recouvrement de désastre, on utilise de plus en plus fréquemment des sites délocalisés, c'est-à-dire physiquement séparés des utilisateurs, de quelques centaines de mètres à plusieurs centaines de kilomètres : plus le site est éloigné, moins il risque d'être touché par un désastre affectant le site de production. Mais la solution est d'autant plus chère, car la bande passante qui permet de transférer des données d'un site vers l'autre est alors généralement plus coûteuse et risque d'être moins performante. Cependant la généralisation des réseaux longues distances et la baisse des coûts de transmission rendent moins contraignante la notion de distance : le coût du site ou la compétence des opérateurs (leur capacité à démarrer le secours rapidement et rendre l'accès aux utilisateurs) sont d'autres arguments de choix.
Les sites de secours (in situ ou déportés) se classent selon les types suivants :
Salle blanche (une salle machine protégée par des procédure d'accès particulières, généralement secourue électriquement). Par extension, on parle de salle noire pour une salle blanche entièrement pilotée à distance, sans aucun opérateur à l'intérieur.
Site chaud : site de secours où l'ensemble des serveurs et autres systèmes sont allumés, à jour, interconnectés, paramétrés, alimentés à partir des données sauvegardées et prêt à fonctionner. Le site doit aussi fournir l'ensemble des infrastructures pour accueillir l'ensemble du personnel à tout moment et permet une reprise d'activité dans des délais relativement courts (quelques heures). Un tel site revient quasiment à doubler les capacités informatiques de l'entreprise (on parle de **redondance**) et présente donc un poids budgétaire non négligeable.
Site froid : site de secours qui peut avoir une autre utilisation en temps normal (ex : gymnase). Les serveurs et autres systèmes sont stockés mais non installés, connectés, etc. Lors d'un sinistre, un important travail doit être effectué pour mettre en service le site ce qui conduit à des temps de reprise long (quelques jours). Mais son coût de fonctionnement, hors période d'activation, est faible voire nul.
Site tiède : site de secours intermédiaire. En général on trouve des machines installées (mise à jour décalée par rapport au site de production) avec les données sur bande mais non importées dans les systèmes de données.
Il est aussi possible d'utiliser des systèmes distribués sur plusieurs sites (diminution du risque de panne par effet de foisonnement) ou un site de secours mobile qui correspond à un camion transportant des serveurs et autres systèmes, permettant de n'avoir besoin que d'un système de secours pour plusieurs sites, en tablant sur l'improbabilité qu'une panne touche simultanément plusieurs sites.
Plus les temps de rétablissement garantis sont courts, plus la stratégie est coûteuse. Il faut donc choisir la stratégie qui offre le meilleur équilibre entre le coût et la rapidité de reprise.

Mesures curatives

Selon la gravité du sinistre et la criticité du système en panne, les mesures de rétablissement seront différentes.

- **La reprise des données**

Dans cette hypothèse, seules des données ont été perdues. L'utilisation des sauvegardes est nécessaire et la méthode, pour simplifier, consiste à réimplanter le dernier jeu de sauvegardes.

Cela peut se faire dans un laps de temps court (quelques heures), si l'on a bien identifié les données à reprendre et si les méthodes et outils de réimplantation sont accessibles et connus.

- **Le redémarrage des applications**

A un seuil de panne plus important, une ou des applications sont indisponibles. L'utilisation d'un site de secours est envisageable, le temps de rendre disponible l'application en cause.

- **Le redémarrage des machines**

VI. Politique de sécurité de l'information

1. Qu'est ce qu'une politique de sécurité de l'information?

Chaque entreprise ou organisme doit se doter d'un ensemble de règles de bon usage et de principes de contrôles visant à protéger ses biens matériels et immatériels (information). Dans le contexte des TIC, la description de ce code de bonnes pratiques et des principes de contrôle s'appelle "politique de sécurité de l'information" (Security Policy). Il s'agit également d'une question de crédibilité face à ses clients, fournisseurs, partenaires et actionnaires ou autorités de tutelle. En incitant les employés à respecter des procédures de sécurité, l'organisation dicte une ligne de conduite en matière de sécurité de l'information et des systèmes informatiques mis en place.

Les politiques de sécurité dérivées de normes reconnues, se déclinent en fonction de deux échelles de recommandations:

- **Light Information Security Policy:** une politique de sécurité de l'information modeste,
- **Reinforced Information Security Policy:** une politique de sécurité de l'information renforcée.

Light Information Security Policy:

Matériel, périphériques et équipement divers

- Fournir une alimentation électrique continue aux équipements critiques.
- Utiliser des modems RTC/ISDN ou des lignes DSL avec précaution: toute transmission d'information critique ou confidentielle via ces systèmes de communication doit être réfléchie si aucun outil de protection (cryptographie) n'est utilisé.
- Contrôler l'infrastructure d'interconnexion informatique (câblage réseau). Toutes les portes d'accès au réseau doivent être identifiées.
- Supprimer les données sur les matériels obsolètes qui ne sont plus utilisés. Les systèmes d'exploitation et applications installés peuvent être conservés.
- Verrouiller chaque station de travail (par exemple via un écran de veille avec verrou) lorsque son utilisateur n'est pas à son poste. Toute station serveur doit impérativement être verrouillée lorsqu' aucun responsable de sa gestion ne l'utilise.

Travail en dehors de locaux de l'organisation et utilisation de personnel externe

- Définir correctement le cadre associé à la mission d'un prestataire de services informatiques externe. Le prestataire de services ne doit avoir accès qu'aux systèmes ou informations qui sont liés aux tâches relatives à sa mission. En outre, le prestataire de services doit garantir la confidentialité des informations qu'il devra manipuler.
- Sensibiliser le personnel quant aux risques liés à l'utilisation d'ordinateurs portables par le personnel.
- Sensibiliser le personnel quant aux risques liés à l'utilisation d'un accès distant (VPN, télétravail, etc.). En effet, le site de travail distant représente une entrée dont le contrôle est plus difficile.

Contrôle de l'accès aux systèmes d'information et aux contenus qui y sont présents

- Mettre en place une méthode d'authentification uniforme, maîtrisée et gérée de manière centralisée. Dans la mesure du possible, il est important de ne pas répliquer les comptes informatiques sur chaque poste de travail.
- **Classifier chaque information mise à disposition sur l'infrastructure informatique et l'associer à des profils d'utilisation.** Chaque profil identifié sera doté d'un ensemble de droits d'accès lui permettant l'usage des informations qui lui sont liées.
- Interdire aux utilisateurs "standards" de s'identifier sur leur poste de travail en utilisant un compte d'administrateur local ou réseau. Si un besoin d'accès à des fonctionnalités "système" est nécessaire (par exemple pour installer un programme), le compte propre à l'utilisateur peut être inséré dans le groupe "administrateurs locaux" de son poste de travail, mais en aucun cas de chaque poste de travail de l'organisation. En outre, le mot de passe de l'administrateur local ou réseau doit obligatoirement rester confidentiel au sein du groupe de gestion informatique.
- Définir une politique de sélection de mot de passe pour les comptes informatiques. Si nécessaire, un compte générique peut être associé à un groupe d'utilisateurs ayant la même fonction. Les mots de passe vides peuvent être tolérés dans certains contextes.
- **Placer les systèmes informatiques sensibles (serveur, router, commutateur, etc.) dans des locaux à accès restreint.** L'accès physique à ces locaux sera limité au personnel autorisé.

Traitement de l'information

- Réserver l'installation et la gestion de l'infrastructure réseau à du personnel qualifié. Une attention particulière sera apportée aux points d'accès sans fil ouverts et aux technologies liées au travail distant (VPN sans firewall interne).
- Réserver tous les actes d'administration système à du personnel qualifié. Faute de personnel qualifié au sein de l'organisation, on fera appel à une entreprise compétente en la matière dans le cadre d'un contrat bien défini.

Messagerie électronique et accès Internet/Intranet/Extranet

- Soumettre tout mail (entrant et sortant) et tout document téléchargé à partir d'une source non fiable (Internet par exemple) à une détection des virus et code malicieux. Un outil de protection doit donc être présent sur chaque poste de travail. Une mise à jour quotidienne de celui-ci est indispensable.
- Utiliser des outils de confidentialité (zip [zip. Format de fichier obtenu après compression] encrypté par exemple) pour l'échange de courriers électroniques concernant des informations sensibles.
- Mettre en place un firewall. Cette mise en place se fera suivant le principe de la fermeture globale de toutes les entrées, suivie de l'ouverture des services requis.
- Traiter avec précaution tout courrier électronique non sollicité.
- Tout document reçu depuis une source non identifiée doit être considéré comme suspect et immédiatement supprimé.
- Vérifier les adresses de destinations lors de l'envoi ou du suivi d'un courrier électronique.
- Envoyer avec discernement les courriers électroniques dont la taille est imposante (plusieurs Mb). Il convient de prendre en compte la capacité de transmission disponible sur le réseau et la capacité potentielle de réception du destinataire afin de ne pas bloquer toute autre transmission.

Reinforced Information Security Policy :

Matériel, périphériques et équipement divers

- Fournir une alimentation électrique continue aux équipements critiques (UPS).
- Prévoir une génératrice de courant comme relais aux UPS.
- Limiter l'utilisation du fax (appareil ou modem) afin de réduire la potentialité de fuite d'information.
- Utiliser des modems PSTN/ISDN ou des lignes DSL avec précaution: toute transmission d'information critique ou confidentielle via ces systèmes de communication doit être réfléchie si aucun outil de protection (cryptographie) n'est utilisé.
- Contrôler l'utilisation des outils d'impression (imprimante locale, imprimante réseau, etc.). Aucune information critique ou confidentielle ne doit être imprimée sans avoir l'assurance que la transmission n'est pas sécurisée. De plus l'utilisation de ressources d'impression distante doit prendre en compte qu'un individu non autorisé peut potentiellement s'emparer des documents imprimés.
- Contrôler l'infrastructure d'interconnexion informatique (câblage réseau). Toutes les portes d'accès au réseau doivent être identifiées et chaque porte non utilisée doit être formellement identifiée, voire même déconnectée.
- Supprimer les données sur les matériels obsolètes qui ne sont plus utilisés.
- Verrouiller chaque station de travail (par exemple via un écran de veille avec verrou) lorsque son utilisateur n'est pas à son poste. Les mesures nécessaires (par exemple un verrouillage automatique après une certaine période d'inactivité) seront mise en place afin de palier un éventuel manquement de l'utilisateur. Toute station serveur doit impérativement être verrouillée lorsqu' aucun responsable de sa gestion ne l'utilise.
- Vérifier lors de la mise en place d'un Intranet/Extranet qu'aucune porte dérobée n'a été ouverte. En effet, une telle faille permettrait le contournement des systèmes d'identification mis en place.

Travail en dehors de locaux de l'organisation et utilisation de personnel externe

- Définir correctement le cadre associé à la mission d'un prestataire de services informatiques externe. Un "Service Level Agreement" doit définir les rôles, droits et obligations auquels le prestataire de service doit se conformer pour garantir le bon fonctionnement des tâches qui lui sont confiées, ainsi que la confidentialité des informations qu'il pourrait être amené à manipuler.
- Contrôler l'attribution des ordinateurs portables au personnel. L'utilisation de cet ordinateur portable doit être restreinte aux seules applications autorisées dans le cadre de la fonction professionnelle. Pour ce faire, une administration système robuste devra être mise en oeuvre sur le système informatique portable afin de garantir que la règle ne peut être contournée. Finalement, les mesures nécessaires (encryption du disque local, droits utilisateur restreints, système d'authentification forte, etc.) devront être mises en oeuvre afin d'assurer la confidentialité de l'information pouvant être disponible en cas de perte ou de vol de l'équipement mobile.
- Contrôler l'accès distant (VPN, télétravail, etc.) par le personnel aux ressources informatiques. Les mesures nécessaires (droits utilisateur restreints, système authentification forte, filtrage du trafic réseau non opportun, etc.) devront être mise en oeuvre afin d'assurer une protection complète de l'antenne distante de l'organisation.

Contrôle de l'accès aux systèmes d'information et aux contenus qui y sont présents

- Mettre en place une méthode d'authentification uniforme, maîtrisée et gérée de manière centralisée. De plus, il est conseillé de pouvoir utiliser cette même infrastructure d'authentification avec les différents systèmes nécessitant une identification d'utilisateur (single sign-on).
- Classifier chaque information mise à disposition sur l'infrastructure informatique et l'associer à des profils d'utilisation. Chaque profil identifié sera doté d'un ensemble de droits d'accès lui permettant l'usage des informations qui lui sont liées. De plus, les informations identifiées comme critiques ou confidentielles feront l'objet de mesures particulières assurant la sécurité nécessaire (encryption de certains contenus sur leur support de stockage et lors de leur transfert sur le réseau de communication, introduction d'un système d'audit de consultation, etc.).
- Associer l'accès aux ressources réseau (imprimante, scanner, unité de stockage, Internet, etc.) à un mécanisme d'identification et d'audit. Le matériel nécessaire aux ressources réseau sera en outre protégé contre des accès en mode direct, c'est-à-dire sans passer par le système de contrôle d'accès (file d'impression sur serveur obligatoire, proxy pour Internet, etc.).
- Réserver les droits "administrateur" aux membres du groupe d'administration informatique. Tous les postes de travail doivent être administrés de telle sorte qu'aucune opportunité d'obtention de tels droits système ne soit possible par du personnel non autorisé. Ceci inclut l'impossibilité pour un utilisateur de modifier (ajout/suppression de programme) la configuration et la stabilité de son poste de travail. De plus chaque poste de travail ne comportera que les applications indispensables à la réalisation des tâches associées à la fonction de l'utilisateur de ce poste.
- Définir une politique de sélection de mot de passe pour les comptes informatiques. Aucun compte générique ne pourra être associé à un groupe d'utilisateurs ayant la même fonction. Les mots de passe vides ne sont pas tolérés et la durée de validité sera déterminée, avec un système de renouvellement forcé. Pour le groupe d'administration informatique, chaque responsable aura son propre compte associé aux droits d'administrateur système et toutes les actions d'administration seront réalisées sous l'identité effective du responsable. De plus, un système d'audit sera mis en place pour permettre la tracabilité des actions réalisées.
- Placer les systèmes informatiques sensibles (serveur, router, commutateur, etc.) dans des locaux à accès restreint. L'accès physique à ces locaux sera limité au personnel autorisé. Le local sera fermé et un mécanisme d'identification (bagde électronique, code personnel, etc.) sera mis en place, de même qu'un système d'audit, si cela est possible. Une attention particulière sera accordée au panneau d'interconnexion réseau (patch pannel). Son accès sera de préférence limité par une armoire fermée réservée aux responsables réseau.
- Réaliser toutes les opérations d'administration distante via des communications sécurisées (par exemple SSH, terminal serveur, etc.). L'objectif est de ne pas transmettre de paramètres d'authentification de compte d'administration en clair et sans protection.

Traitement de l'information

- Réserver l'installation et la gestion de l'infrastructure réseau à du personnel qualifié. Aucune connexion à l'infrastructure ne doit être possible sans l'intervention du personnel responsable (filtrage d'adresse ethernet MAC [MAC (Media Access Control). Adresse qui est associée à une interface qui se situe au niveau de la couche liaison de données, comme le protocole ethernet. Cette adresse identifie univoquement l'interface au sein d'un réseau local], désactivation des portes non-utilisées sur le commutateur, instauration de règles de filtrage firewall pour le trafic interne à l'organisation, etc.). En outre tout ajout de systèmes de communication sans fil (WiFi) devra être associé à une encryption forte (WPA et non WEP) et les accès distants (VPN) seront soumis à un contrôle strict. Enfin, tout matériel de communication n'étant pas sous le contrôle total du gestionnaire sera proscrit (par exemple un modem sur les stations de travail).
- Réserver l'administration "système" à du personnel qualifié appointé par l'organisation.
- Enregistrer toute tentative d'accès infructueux à des documents ou au système d'information (log [log (log file, fichier log). Fichier généré par le serveur contenant l'ensemble des informations relatives à un site Web, notamment pour sa fréquentation (hits, pages vues, visiteurs, etc)]).
- Analyser à intervalles réguliers les enregistrements des fichiers de logs (access log, error log, authorisation log, etc.). Cette analyse sera réalisée par du personnel compétent. En outre, il est indispensable que chaque système informatique synchronise son horloge avec une horloge de référence (serveur ntp).

Messagerie électronique et accès Internet/Intranet/Extranet

- Soumettre tout mail (entrant et sortant) et tout document téléchargé à partir d'une source non fiable (Internet par exemple) à une détection des virus et code malicieux. Un outil de protection doit donc être présent sur chaque poste de travail. En outre, une centralisation de la gestion de ces outils doit impérativement être réalisée par les responsables informatiques et la mise à jour du logiciel doit être impérativement réalisée plusieur fois par jour.
- Réaliser les échanges de courriers électroniques concernant des informations et documents à caractère sensible au moyen d'outils permettant l'encryption des messages suivant un système à clé publique/clé privée. Tout échange de ce type devra en outre être associé à une signature électronique. L'administration des certificats se réalisera d'une manière centralisée par les gestionnaires informatiques.
- Vérifier lors de la mise en place d'un Intranet/Extranet qu'aucune porte dérobée n'a été ouverte. Avant toute mise en place d'un Extranet, une ingénierie des communications réseau doit être réalisée afin de restreindre l'accès aux ressources exclusivement internes à l'organisation à des partenaires disposant des droits d'accès suffisants. De plus, un système d'audit doit être mis en place.
- Mettre en place un firewall. Cette mise en place se fera suivant le principe de la fermeture globale de toutes les entrées, suivie de l'ouverture des services requis. Le firewall devra être de type "statefull" et les messages de notification enregistrés et conservés (syslog [Syslog. Service réseau offrant des facilités de collecte de logs informatiques. Ce service permet une centralisation de toutes les sources d'informations de logs, ce qui autorise une meilleure administration "système»]).
- Traiter avec précaution tout courrier électronique non sollicité. L'administration informatique devra mettre en oeuvre des outils (filtre anti-spam) au niveau du serveur de courrier afin de minimiser au maximum ce type de sollicitations.

- Tout document reçu depuis une source non identifiée doit être considéré comme suspect et immédiatement supprimé. La direction informatique doit en être informée.
- Vérifier les adresses de destinations lors de l'envoi ou du suivi d'un courrier électronique.
- Mettre en place des systèmes évitant l'envoi de courriers électroniques de grande taille. Ces messages pourraient en effet bloquer toute autre transmission. C'est l'administration informatique qui est chargée de cette tâche (par exemple via une règle sur le serveur de courrier).
- Mettre en oeuvre des outils d'analyse réseau (par exemple IDS) afin d'identifier tout trafic ou comportement anormal. C'est l'administration informatique qui est chargée de cette tâche.

2. Méthodes

Il existe de nombreuses méthodes permettant de mettre au point une politique de sécurité. Voici une liste non exhaustive des principales méthodes :

- MEHARI (MEthode Harmonisée d'Analyse de Risques) ;
- MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) ;
- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) ;
- La norme ISO 17799
- ….

MEHARI

La méthode MEHARI est une méthode d'analyse des risques. Elle a été conçue pour être adaptable au contexte de l'entreprise (boîte à outils avec possibilité d'adapter la démarche) mais elle ne dispose pas de déclinaison par typologie d'entreprise ou métier.

MEHARI existe en Français et en Anglais et est maintenue par le CLUSIF (club de la sécurité des systèmes d'information français). Elle est dérivée des méthodes Marion et Melisa (qui eux n'évoluent plus depuis plusieurs années). MEHARI est utilisée par de nombreuses structures publiques et privées en France mais également au Québec.

MEHARI se nourrit des enjeux et des objectifs de l'entreprise afin de livrer un résultat « business » quant aux mesures de sécurité à mettre en ouvre. Les différentes phases sont d'établir le contexte d'entreprise, d'identifier les actifs et les menaces, d'analyser les risques et enfin de définir les mesures de sécurité (traitement du risque).

La méthode MEHARI a été conçue pour les grandes entreprises et organismes (qui sont également les principaux demandeurs de méthodologie de risques) et prévoit la démarche de sécurité de l'information à 2 niveaux :

- Niveau stratégique : niveau liée au(x) métier(s) de l'entreprise et indépendantes des processus et technologies mis en ouvre. Ce niveau fixe les objectifs de sécurité et le métrique des risques.
- Niveau opérationnel : entité, filiale, branche, business unit qui met en ouvre cette politique et la décline en analyse précise des risques, définition des mesures de sécurité à mettre en ouvre et pilotage de la sécurité dans le temps (contrôles et tableaux de bord)

Cette « architecture » de MEHARI à deux niveaux est bien adaptée pour des grands groupes qui veulent conserver une cohérence entre entités (exemple banque internationales).

Un logiciel de gestion des risques **Risicare** (de la société BUC SA) est proposé en complément de la méthode MEHARI pour élaborer des représentations graphiques, des tableaux de cotations, des moyens de reporting et une assistance à la méthode. Cet outil, si il est bien utilisé, permet de simplifier une analyse MEHARI et ainsi d'être intéressant pour les moyennes entreprises.