Dossier de Sécurité d'une STA

Par Florian LE BRAS BTS SIO1

Introduction

Tout d'abord il faut savoir qu'il n'existe pas de système informatique totalement sécurisé mais il y a quelques mesures simples à mettre en place permettent de se sécuriser un minimum :

- Sauvegarde de ses données pour éviter les pertes.
- Utilisation d'un pare-feu
- Essayer les plus possibles d'effectuer les mise à jours de son système d'exploitation et de ses applications.
- Installation de logiciels de protection
- Les menaces
- Cependant même avec toutes ces mesures c'est vous qui devait être attentif

<u>Sauvegarde de ses données pour éviter les pertes.</u>

Il n'est pas inutile de vous rappeler qu'il est important d'effectuer un « backup » pour ses données pour éviter les mauvaises surprises. On a tous déjà perdu des données à cause d'une mauvaise manipulation, d'une panne, d'un piratage ou d'un vol. Il suffit d'un instant pour voir vos travaux, photos, sons, vidéos disparaitre dans le néant. Dans ce cas il y a deux solutions soit vous les avez sauvegardés ailleurs soit vous les avez perdus.

Il y a plusieurs solutions pour sauvegarder ses données :

1. La sauvegarde physique
2. En réseau
3. Dans le Cloud

1. **<u>La sauvegarde physique :</u>**

La solution la plus évidente c'est de faire une copie de sauvegarde locale (utiliser un disque de secours). Il est préférable de privilégier les disques durs externes aux internes car il est plus simple de compréhension et on peut emporter tous nos données avec nous comme une clé USB. Pour optimiser encore plus on peut utiliser un logiciel de synchronisation comme SyncBack qui va permettre de sauvegarder de manière régulière et automatique toutes vos données.

2. **<u>En réseau :</u>**

Le problème avec les disques de secours c'est qu'au bout d'un moment on se retrouve a utiliser plus disques durs, plusieurs appareils, et là, on s'y perd. C'est là qu'intervient la solution en réseau qui va permettre de créer un espace de sauvegarde de données entre plusieurs machines. Là on a deux solutions :

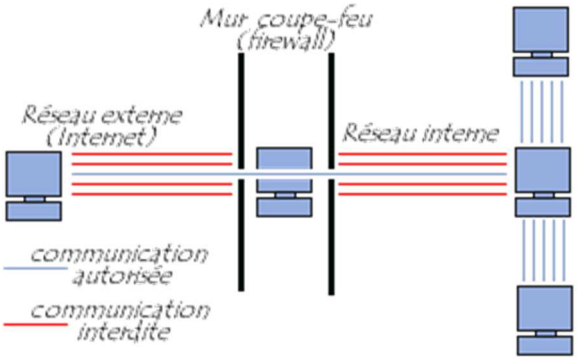
- Créer un serveur FTP sur une seconde machine mais c'est très compliqué à réaliser.
- Achetez un NAS (Network Attached Storage) qui est beaucoup plus simple (150~300 €)

3. **<u>Dans le Cloud :</u>**

Et pour finir la solution la plus facile : stocker dans le Cloud. Ils en existent une multitude comme Box encore DropBox. L'avantage de cette solution c'est qu'on peut synchroniser nos données en permanence, la prise en main est très facile et on peut partager nos données avec d'autre personne grâce à un lien. Les prix changent en fonctions de stockage, gratuits pour 20 ou 30 Go en moyenne et au-delà il faudra payer. (20~100€)

Utilisation d'un pare-feu

Chaque ordinateur connecté à internet peut être pris pour cible d'une attaque informatique.
Le pare-feu va servir de mur, il va filtrer les paquets de données échangés avec le réseau.
Il a au minimum 2 interfaces, une pour le réseau interne qui vaut protéger et une pour le réseau externe (ex : Internet)



Le système firewall est un système qui constitue l'intermédiaire entre le réseau interne et externe. Il est possible d'en mettre sur n'importe quelle machine pourvu que le pc soit assez puissant et le système sécurisé

Le filtrage des paquets

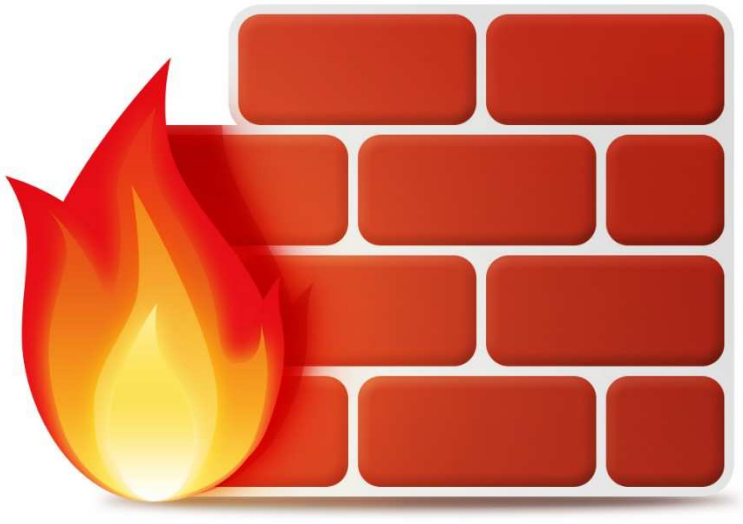
Le firewall analyse les en-têtes de chaque paquet de données échangé entre une machine interne au réseau et une machine extérieure.

Les en-têtes sont constituées de :

Action	**IP source**	**IP destinataire**	**Protocol**	**Port source**	**Port destinataire**

Comme exemple :

Accept	192.168.10.20	194.154.192.3	tcp	any	25
Deny	any	any	any	Any	Any



Mise à jour de son système d'exploitation et de ses applications

Les systèmes d'exploitation et les applications ont de nombreuses failles mais celles-là sont souvent corrigées cependant pour que l'a correction de cette faille s'exécute il faut alors faire la mise à jour.C'est pourquoi il est très important que votre système d'exploitation soit toujours à jour. Pour cette raison, Microsoft vous explique que vous devez posséder une licence achetée de Windows pour faire ces mises à jour. Dans le cas contraire votre machine sera insuffisamment protégé et vous de contaminer involontairement d'autres personnes en laissant les choses en l'état.

Les logiciels de protection

Pour protéger son poste, il est important d'utiliser des logiciels qui permettent d'empêcher toute action nuisible et neutraliser si nécessaire un programme. Les logiciels principaux utilisés sont ;

1. L'anti-virus

Un anti-virus est un programme qui empêche les virus de contaminer votre ordinateur. Le rôle principal d'un anti-virus est d'empêcher l'arrivée d'un virus sur la machine. Si un virus a réussi à pénétrer dans le système, l'action de l'anti-virus sera beaucoup moins efficace.

En parlant d'efficacité l'anti-virus doit être présent sur la machine **avant** toute source de contamination, être à jour (voir importance des mises à jour) et être actif en permanence.

Lorsque l'anti-virus détecte un fichier infecté il va vous demander soit de le supprimer (tout le fichier), supprimer le code infecté ou de mettre en quarantaine le fichier infecté.

2. bloqueur de logiciel espion (spyware)

La principale difficulté avec les spywares est de les détecter. La meilleure façon de se protéger est encore de ne pas installer de logiciels dont on n'est pas sûr à 100% de la provenance et de la fiabilité. Cependant il existe tout de même des logiciels anti-spyware gratuits et facilement accessible. Les plus connus sont AdwCleaner ou encore Malwarebytes Anti-malware.

3. Bloquer de pub

Les bloqueur de pubs intempestives peuvent être installés pour empêcher les pop-up. De nombreux navigateurs WEB comportent par défaut, un blocage de pub. Mais cependant le plus connu est Adblock qui est un module qu'on rajoute au navigateur pour éviter les fenêtres publicitaires encombrantes.

Les menaces

On sait comment se protéger mais se protéger de quoi ?

Les virus il y en a des multitudes qui existent et d'autre qui n'existent pas encore mais voilà les plus connus :

Les vers informatiques : Il se différencie des virus classiques car ils se propagent aux travers des réseaux et il est capable de se répandre rapidement. Il est utilisé par les pirates pour de l'espionnage, du vol de données, ouvrir des portes dérobés et ainsi permettent le contrôle de la machine infectée.

Les chevaux de Troie : Il est sans doute le virus le plus connu. Tout le monde connait l'histoire du cheval de Troie dans la mythologie Grecque. Pour qu'il s'active il faut que l'utilisateur autorise le logiciel malveillant à s'installer. Ils sont à l'instar des vers très dangereux car ils permettent aussi d'ouvrir des portes dérobés et ainsi permettent le contrôle de la machine infectée, du vol de donné mais ils permettent aussi d'installer des logiciels malveillants. Mais contrairement aux vers ils ne se dupliquent pas.

Les rootkits : Il regroupe un ensemble de techniques pour ouvrir et maintenir un accès via le réseau à une machine en toute invisibilité. Il peut permettre de dissimulé des virus ou autres chevaux de Troie. Il est très difficile à détecter mais de plus en plus d'anti-malware intègre une détection des rootkits.

Les rogues : Le rogue est un faux logiciel de sécurité comme un anti-virus. Il va envoyer à l'utilisateur un message de présence d'infections (fausse) importante et propose de la traité moyennant de l'argent. Ce logiciel est totalement inutile car la menace est fictive.

Les spywares : Les spywares est un logiciel espion. Il s'installe sur un poste pour collecter un maximum d'informations. Il peut être utilisé pour de la pub ciblé mais aussi pour récupérer des mots de passe ou des codes d'accès. Ils se propagent par messagerie mais aussi par téléchargement et navigation sur des sites à contenu douteux voire illégales.

Les virus : C'est un bout de programme introduit dans un autre programme et au démarrage de ce dernier il va s'activé ; il a donc besoin de l'intervention de l'utilisateur pour se propager. Il y aussi d'autres formes de virus les virus de boot (s'intègre pas à un fichier mais au secteur de démarrage d'un support comme une clé USB ou un disque dur), les macro-virus (Ils ne se propagent que par des fichiers Microsoft-Office ils peuvent se propager par un simple échange de document Word) et les virus-vers (C'est la combinaison entre un virus et un vers. Ils sont capables de se propager sur un réseau mais nécessite un programme hôte).

Le spam : Ce sont des courriers à but publicitaire envoyés en masse à des milliers d'internautes qui n'ont pas donné leur accord. Ils représentent 50% du trafic de mail et dévalorise les démarches responsables.

Machines zombies : C'est une machine qui est contrôlé à l'insu de son utilisateur par un pirate. Ce dernier va l'utiliser pour attaquer d'autre machines en se cachant derrière cette machine.

L'homme du milieu : C'est une attaque qui va intercepter les communications entre deux machines sans qu'aucune ne s'en rendent compte. Il peut modifier les communications.

Le phishing : Le phishing ou le hameçonnage est un style de piratage qui envoie un mail à client qui contient un lien d'un faux site (souvent banque). Il ressemble au site d'une banque il va vous demander de donner vos comptes bancaires et ainsi les récupérés.

Le piratage psychologique : C'est la méthode la plus facile pour les pirates car il consiste à exploiter le comportement humain. Le pirate se fait passé pour un responsable du réseau, un chef d'entreprise et demande des données à un employeur par exemple, celui-ci va donc, pensant s'adresser à son supérieure, donner les données.

L'importance de l'utilisateur

Comme on peut voir dans les menaces l'utilisateur à une part importante de la sécurisation d'un poste. Il a quelques mesures simples à mettre en place pour mieux sécuriser son PC. Il doit mettre un mot de passe sur son ordinateur (très important sur un pc portable). Il doit avoir un comportement sans risque, éviter des sites internet suspects, de télécharger des logiciels douteux. Il ne doit pas diffuser son adresse mail ou autre donnée personnelle sur n'importe quel site pour éviter les spams inutiles car si votre messagerie est remplie de spam c'est que votre adresse circule sur Internet. Ne pas répondre à des mails de personnes inconnus car souvent derrière ce mail se cache un pirate qui cherche à contaminer une machine.

Pour conclure tous les logiciels sont un cadenas mais c'est vous qui avez les clés.