SE PROTÉGER

Intrusions

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable. Lorsqu'on surfe sur le Net, on s'expose à certains dangers. Il est indispensable de connaître les principaux types d'attaques afin de mieux s'en protéger.

Le virus

Petit logiciel se dupliquant par ses propres moyens sur un même ordinateur et se propageant d'ordinateurs en ordinateurs et dont le but est d'occasionner des dégâts : perte de données, ralentissement de la machine, ...

Les virus se transmettent via les mails, les chats, les messageries instantanées et via les supports d'enregistrement des données (clé USB, disque amovible).

Le spyware

Logiciel espion qui surveille vos habitudes de navigation sur Internet et qui collecte des informations souvent à des fins de marketing à votre insu. Le spywares peut aussi être une source de nuisances diverses : consommation de mémoire vive, utilisation d'espace disque, mobilisation des ressources du processeur, ...

Il s'installe sur votre machine via les mails, le surf sur internet, l'installation de programmes.

Le trojan (cheval de Troie)

Programme qui récolte des informations personnelles et effectue des opérations nuisibles sans l'autorisation de l'utilisateur : lecture, modification, suppression, récupération de fichiers,... Il se différencie du virus par le fait qu'il ne se reproduit pas. Le trojan crée également des failles dans votre ordinateur. Ces failles permettent à des pirates informatiques de prendre le contrôle de votre machine.
Le trojan s'implante sur votre machine via les mails, les téléchargements, la navigation sur Internet

Pour réduire ces risques d'intrusion sur votre ordinateur, il existe des outils :

Les anti-virus

Logiciel qui vérifie en permanence les fichiers de votre ordinateur pour s'assurer qu'ils ne contiennent pas de virus. **Exemples** : Avira Antivir (gratuit), Security Essentials (antivirus gratuit de Microsoft), BitDefendre (payant et gratuit).

Les anti-spywares

Logiciel qui regarde si d'autres logiciels n'espionnent pas votre activité ou ne transmettent pas certaines de vos données confidentielles. **Exemples** : Lavasoft Adaware (version gratuite et version payante), Malwarebytes (gratuit), Spybot (gratuit).

Firewall

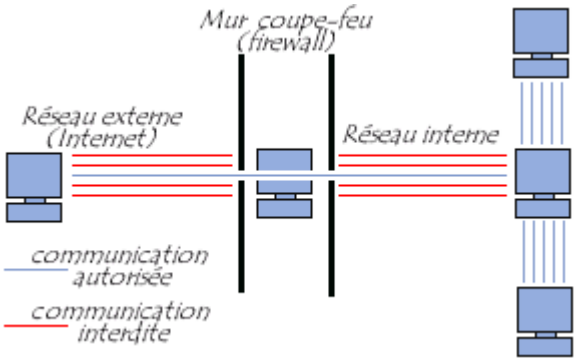
Qu'est-ce qu'un pare-feu ?

Chaque ordinateur connecté à internet est susceptible d'être victime d'une attaque d'un pirate informatique. Les pirates informatiques scrutent le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis cherchent une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant.
Ainsi, il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes qui possèdent une connexion internet de se prémunir contre ces intrusions en installant un dispositif de protection.

Un pare-feu est un logiciel ou un matériel qui vérifie les informations provenant d'Internet ou d'un réseau, puis les empêche d'accéder à l'ordinateur ou les y autorise, selon vos paramètres de pare-feu définis.

Les pare feu filtrent les données essayant d'entrer sur votre ordinateur afin de ne pas laisser entrer des données pouvant affecter votre ordinateur et éviter ainsi le piratage informatique.

Le pare-feu sert d'interface entre votre ordinateur (réseau interne) et internet (réseau externe) et empêche certains transferts de données potentiellement dangereux entre votre ordinateur et internet.
A l'origine, les pare-feu servaient à protéger des réseaux d'ordinateurs et étaient installés sur des ordinateurs particuliers au sein d'un réseau.



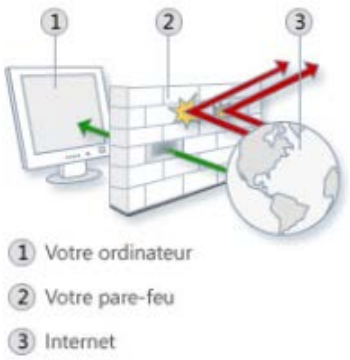
Aujourd'hui, de nombreux ordinateurs possèdent leur propre firewall. On parle de pare-feu personnel. Le firewall personnel est un logiciel qui fonctionne directement sur l'ordinateur à protéger.
L'avantage d'un pare-feu personnel est qu'il peut empêcher les attaques du type cheval de Troie, c'est-à-dire l'installation automatique de programmes nuisibles ouvrant une brèche dans le système afin de permettre à un pirate informatique de prendre la main à distance sur la machine.

Typiquement, un firewall permet à votre ordinateur de se connecter à internet mais bloque les tentatives de connexion d'internet vers votre ordinateur.

Attention : Un pare-feu n'est pas la même chose qu'un antivirus. Pour protéger votre ordinateur, vous devez disposer d'un pare-feu et d'un logiciel antivirus contre les programmes malveillants.

Comment ça marche ?

Le schéma suivant illustre la façon dont un pare-feu fonctionne. À l'image d'un mur en brique capable de créer un obstacle physique, un pare-feu crée un obstacle entre Internet et votre ordinateur.
Un système pare-feu contient un ensemble de règles prédéfinies permettant de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par le système. 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 est aussi la plus contraignante, car elle demande d'identifier quelles sont les communications autorisées.

En suivant ces règles, le pare-feu va 1/ autoriser une connexion, 2/ bloquer la connexion ou 3/ rejeter la demande de connexion sans avertir l'émetteur.

Où se procurer un pare-feu ?

À savoir : Windows dispose d'un pare-feu Windows. Vous le trouverez dans le panneau de configuration de votre ordinateur.

En savoir plus : site Microsoft
Voici quelques pare-feu personnels de référence :

- Zone Alarme
- Comodo Firewall pour Windows
- Kerio Personal Firewall
- Sygate personal firewall

Sources :

- http://www.commentcamarche.net/contents/992-firewall-pare-feu
- http://sebsauvage.net/comprendre/firewall/
- http://windows.microsoft.com/fr-be/windows/what-is-firewall#1TC=windows-7