PrimaryCare

La sécurité sur Internet – 3e partie: Firewall

Angel Vilaseca

Après avoir décrit les menaces, voici un moyen de se protéger: le *Firewall.*

Un firewall – traduisez «cloison pare-feu» – est un terme imagé, qui dit bien ce qu'il veut dire. Il s'agit d'un programme informatique qui filtre le trafic des données entrant ou sortant de votre ordinateur.

Lorsque votre ordinateur est connecté à Internet, de l'information entre et sort constamment par ses «ports». Un ordinateur possède des milliers de «ports». Il s'agit de passages virtuels par lesquels de l'information transite dans et hors de votre ordinateur.

Une partie de cette information va de soi pour vous, par exemple quand vous:

– envoyez et recevez des e-mails,
– visitez un site web,
– remplissez un formulaire virtuel sur un site,
– téléchargez des fichiers.

Toutefois, il y a aussi de l'information qui entre et sort de votre ordi sans que vous le sachiez, par exemple votre copie de Windows ou d'autres programmes qui vont voir automatiquement sur le website du fabricant s'il y a des mises à jour disponibles. En général, ces échanges d'information invisibles ont lieu pour une bonne raison. Mais parfois ils peuvent être utilisés par des pirates.

Cette propriété permet que votre ordinateur puisse être infecté par un programme malfaisant. Il suffit qu'il soit connecté à Internet, rien d'autre. Dans le temps, il fallait, pour que l'ordinateur soit contaminé, cliquer sur la pièce jointe d'un e-mail piégé. Ce n'est désormais plus nécessaire. Le seul fait d'être connecté à Internet suffit.

En août 2003, on en a eu un bon exemple avec le virus *Blaster*, qui plantait l'ordinateur environ une minute après l'avoir allumé.

Si on connecte un ordinateur à Internet, en laissant ses ports ouverts, sans les monitorer, on dit qu'à l'heure actuelle, après seulement une vingtaine de minutes, il y aura au moins une des bébêtes de la liste ci-dessous qui va s'y intéresser.

Quelques définitions

Virus: Il s'agit de programmes ou de morceaux de code informatique qui vont aller infecter un ou plusieurs programmes sur votre PC. Les programmes infectés se comportent de façon inhabituelle et peuvent parfois faire planter l'ordinateur.

Vers (Worms): Le but de ce type de virus est de se reproduire autant que possible dans un réseau, allant jusqu'à le saturer. Plus dangereux qu'un virus, car dans ce cas ce n'est plus un seul ordinateur, mais tout un réseau, voire même théoriquement tout l'Internet qui plante.

Port scanning: Un hacker peut passer en revue tous les ports de votre ordinateur, pour voir s'ils sont ouverts, voire même s'ils existent. Si votre PC communique et qu'un de ses ports est ouvert, le hacker peut y envoyer un virus ou un ver. Il peut même se servir d'un port ouvert pour prendre le contrôle de votre ordinateur.

Cookies: Il s'agit de petits fichiers de données, placés dans votre ordinateur par un site web que vous avez visité. Un cookie peut conserver vos données personnelles, que vous avez données sur le site. Par exemple, si vous donnez votre numéro de carte de crédit, le cookie peut le conserver jusqu'à la prochaine fois que vous voudrez acheter quelque chose sur ce site précis. Ainsi vous n'aurez plus à sortir votre carte de crédit et mettre vos lunettes pour en lire le numéro puis le taper laborieusement sans faire d'erreur. C'est pratique, c'est une bonne idée et la plupart des sites commerciaux de la Toile utilisent cette propriété de façon tout à fait légitime ... Mais parfois pas!

Chevaux de Troie: Il s'agit de programmes d'aspect tout à fait rassurant, mais qui font quelque chose d'illégitime quand on les met en route. Admettons que vous téléchargiez un programme intéressant, offert gratuitement sur Internet mais vous ne savez pas qu'il est piégé. C'est en réalité un Cheval de Troie. Vous l'installez sur votre PC et vous le mettez en route. Sans que vous le sachiez, il va aller ouvrir des ports du PC à l'intention de hackers, transmettre des mots de passe ou des numéros de carte de crédit, ou encore détruire vos fichiers. Un cheval de Troie (Trojan) est aussi un type de virus mais en général, il ne se reproduit pas.

Attaque de type Denial Of Service (DOS): Rien a voir avec DOS (Disk Operating System) l'ancien système d'exploitation des PC qui a été remplacé par Windows. Lorsqu'un hacker trouve un port de votre PC ouvert, il peut l'attaquer en lui envoyant une énorme quantité de données, de manière à le saturer. Le port n'arrive pas à accepter autant de données, les ressources du système s'épuisent et le PC plante, en d'autres termes, il refuse de fournir ses services (Denial of Service).

* Der Ärztegrossist Zur Rose hat ein Artikel-unabhängiges Sponsoring für die Rubrik «Medizinische Informatik» übernommen. Die Beiträge in dieser Rubrik entstehen vollkommen unabhängig von diesem Sponsoring und durchlaufen den normalen redaktionellen Review-Prozess. Durch die direkte Beteiligung an den Produktionskosten ermöglicht das Rubrik-Sponsoring die kostenlose Zustellung von PrimaryCare an alle Hausärztinnen und Hausärzte in der Schweiz. Die Herausgebergesellschaften und die Redaktion danken der Firma «Zur Rose» herzlich für ihre Unterstützung.

Spyware et hardware ont été décrits dans un précédent article. Ces programmes sont placés dans votre PC à votre insu et transmettent à leurs maîtres des informations sur vous et votre PC.

Firewall

Le firewall va donc filtrer tout cela, en se basant sur les critères que vous lui donnerez. Il possède les possibilités suivantes:

- rendre votre PC invisible sur l'Internet. Les ports de l'ordinateur ne sont pas seulement fermés, ils n'existent même plus, vus depuis Internet;
- bloquer automatiquement tout trafic suspect;
- vous alerter chaque fois qu'un programme dans votre PC essaie d'envoyer de l'information à un autre ordinateur. Cela empêchera les chevaux de Troie, spywares et adwares d'envoyer des informations confidentielles à des personnes malintentionnées.

Plus d'autres choses, d'un niveau plus technologique. Un firewall s'impose d'autant plus si vous possédez un accès Internet à haute vitesse (ADSL). En effet, un tel PC est une cible de choix pour un hacker car il va lui permettre de commettre ses forfaits d'autant plus rapidement et à plus grande échelle que le débit de la liaison Internet est plus élevé.
De plus, un utilisateur paie sa liaison ADSL par forfait, qu'elle soit utilisée ou non, et non pas selon le temps passé à communiquer, ce qui était le cas des anciens modems. On peut donc laisser la liaison ADSL always on, c'est-à-dire que l'ordi est relié en permanence à Internet, sans que cela coûte davantage à l'utilisateur.
Il peut arriver qu'un hacker prenne le contrôle de votre ordi pour par exemple envoyer pendant des heures entières, et à votre insu, des spams à des milliers de personnes tout en simulant que c'est vous qui en êtes responsable. Suivant le contenu des spams, cela risque éventuellement de vous attirer quelques ennuis. Alors prudence! Equipez-vous.

Dr Angel Vilaseca
8, pl. du Rondeau
CH-1227 Carouge
avilaseca@bluewin.ch