Fiche pratique

Les risques du réseau

La protection d'un réseau au sens de la défense contre les intrusions nécessite un matériel spécifique dont c'est l'unique fonction : le pare-feu (firewall en anglais). Il faudra néanmoins veiller à paramétrer correctement chaque élément du réseau (ordinateurs, serveurs) afin qu'aucun d'entre eux ne soit une faiblesse dans la muraille. Enfin il faudra s'assurer de la bonne protection des ordinateurs au niveau des systèmes d'exploitation et des logiciels, mais c'est encore une autre histoire...

Le pare-feu est un matériel (ou un logiciel) qui fonctionne le plus simplement du monde. Il agit comme un filtre qui laisse passer uniquement les données dont il peut identifier la provenance ainsi que la destination et ce, à l'unique condition que cela n'entre en contradiction avec aucune règle. Sa fonction est donc de rendre hermétique le réseau local privé aux éléments extérieurs non désirés. Un pare-feu correctement paramétré fonctionne sur le modèle du « refuse tout, sauf exception ». Cela signifie qu'il n'accepte aucune communication en provenance de l'extérieur sauf celles qui correspondent à une liste d'exceptions définies par l'administrateur. Quand on parle de laissez-passer il s'agit simplement d'accepter de transmettre les données au réseau local.

Un routeur ?

Tout comme le routeur, le pare-feu matériel possède deux « pattes ». L'une branchée sur le réseau interne et l'autre sur le réseau externe. Dans votre box, cela vous est invisible mais d'un côté il est branché sur l'élément routeur et de l'autre sur l'élément switch. Si une demande arrive de l'extérieur, il vérifie sa validité et si celle-ci est avérée il envoie la demande au réseau interne. Dans l'autre sens il laisse tout passer en général. Il est toutefois possible de lui demander de ne pas laisser passer les données qui transitent sur un port en particulier.

Cela n'est donc pas un routeur puisque sa fonction n'est pas de relier deux réseaux mais il en a les caractéristiques extérieures.

A la maison

Vous allez me dire que vous ne voyez pas bien en quoi vous seriez susceptible d'être attaqué, vous qui ne recelez aucune donnée bancaire ou sensible... Détrompez-vous, les ordinateurs les plus attaqués sont bien ceux des particuliers qui sont les plus nombreux sur la toile et qu'on peut très facilement utiliser pour constituer une gigantesque « armée » dans le cadre d'une attaque par déni de service. Ce genre d'attaque suppose d'avoir infiltré un très grand nombre d'ordinateurs au moyen d'un ver informatique et de leur commander à un instant précis d'effectuer une demande de connexion sur un serveur en particulier. Aucun serveur n'est calibré pour recevoir des centaines de milliers voire des millions de demandes simultanées et dans ce cas les ressources de celui-ci sont très vite épuisées et il cesse de fournir son service jusqu'à ce qu'on le redémarre.

C'est une chose de ne pas participer à une guerre informatique car qui sait votre ordinateur servira peut-être demain à attaquer des serveurs d'un pays ou d'une entreprise. Le mieux est quand même de tâcher d'éviter cela... C'en est une autre de vouloir mettre en sécurité ses fichiers informatiques. Les photos sont par exemple un bien rare mais leur perte est facilement surmontable. Les données bancaires et les fichiers « intimes » sont beaucoup plus délicats de ce point de vue. Il est préférable de ne pas les laisser entre toutes les mains et c'est ce qui arriverait si votre box n'était pas équipée d'un pare-feu pour empêcher quiconque de s'introduire sur votre réseau.

Mots clés :

- Pare-feu
- Firewall
- Box
- WLAN
- Wi-Fi
- Sécurité
- Intrusions

Page suivante >

Mais encore ?

Malheureusement le tableau n'est pas encore tout à fait complet puisque nous ne sommes pas encore revenus sur les réseaux sans fil. Nous avons déjà vu à plusieurs reprises qu'un réseau WLAN (Wi-Fi) est accessible à une distance non négligeable de votre domicile et que sa sécurité est toute relative. Pour certains il suffit de cinq minutes pour s'y introduire, pour d'autres c'est une question de semaines... et de détermination... quoi qu'il en soit une fois sur votre réseau le pirate aura déjoué toutes les protections réseau qui existaient. Il y a une chose importante à savoir c'est que le pare-feu n'intervient que pour les communications extérieures à votre réseau. Si une personne s'est introduite sur votre réseau sans fil sans que vous le sachiez, elle ne rencontrera aucun obstacle pour entrer en communication directe avec tous les équipements de votre réseau. Plus grave, pour les possesseurs de box Wanadoo/Orange, il aura aussi accès automatiquement et sans authentification à tous vos e-mails Orange ainsi que tous vos paramètres de connexion, d'abonnement etc... Il pourra les changer et pourquoi pas vous exclure de votre propre réseau.

Ceci est un élément capital de la sécurité de votre réseau : le paramétrage de votre box. Seulement cinq minutes suffisent pour mettre en place une sécurité satisfaisante et dormir tranquille. Je vous invite à consulter les fiches documentaires spécifiques à votre fournisseur d'accès pour savoir comment faire. Ensuite revenez-vite car il faut que je vous parle de la sécurité de votre ordinateur !

Repères :

Toutes les box sont aujourd'hui équipées d'un pare-feu (ou firewall). Ce dispositif sert à filtrer les informations sortantes (upload) mais surtout les informations entrantes (download), c'est à dire d'un réseau extérieur comme Internet vers votre réseau interne, votre ordinateur : affichage de pages web, réception d'e-mails, téléchargement de fichiers, etc. Le pare-feu peut ainsi détecter des anomalies et refuser l'entrée de certaines données, vous empêchant ainsi d'être la proie d'un pirate ou d'un ver.

Un pare-feu correctement configuré est donc important. Toutefois, l'individu qui voudra s'introduire sur votre réseau pourra aussi le faire via le signal Wi-Fi que vous émettez en permanence, s'il est à sa portée. Et s'il y parvient, il ouvre la caverne d'Ali Baba...

Une configuration minimum de votre box vous permettra de paramétrer à la fois votre pare-feu et votre Wi-Fi, alors continuez de lire les conseils Panoptinet, et prenez de bonnes résolutions !