Fiche pratique

La sécurité

La sécurité est un sujet très vaste car il touche aux sept couches du modèle OSI dont nous avons parlé à de nombreuses reprises. Si on ajoute à cela un huitième niveau qui serait l'utilisateur lui-même, cela nous donne un grand nombre d'éléments à surveiller pour faire en sorte que son réseau soit sécurisé. Certains sont paramétrables, d'autres ne dépendent pas de vous. Dans ces fiches vous apprendrez à paramétrer correctement ce qui est configurable et à adopter les bons comportements qui permettent de réduire le risque à sa portion congrue. En effet, ne croyez pas que vous pourrez bâtir une forteresse ! Il y a un équilibre à trouver entre la valeur de ce que vous voulez protéger et les moyens que vous y consacrerez. Pour bien comprendre les clés de tout cela il vous faudra avoir les connaissances minimales apportées par les fiches théoriques et surtout vous débarrasser d'un grand nombre de préjugés et de ce que nous partageons tous : une certaine paresse.

Mots clés :

- Sécurité
- Hadopi
- Peer-to-peer
- QCM

Un antivirus ne protège pas des virus

Derrière cette phrase un peu provocante, il y a un message simple : l'antivirus le plus efficace est vous-même. Et un antivirus sera bien incapable de vous protéger si vous téléchargez de manière inconsidérée des fichiers sur eMule sans mesurer le risque lié au fichier sur lequel vous cliquez. Dans bien des cas les virus arrivent téléchargés sur eMule parce qu'on croyait prendre un mp3 sans avoir considéré que le fichier en question avait une taille de 100Ko. Le corollaire à tout cela est que pour ne pas attraper de virus il faut savoir le mieux possible ce que l'on fait. Ici nous n'apprendrons pas à télécharger sur eMule mais toutes les informations que vous obtiendrez sur ce site vous donnerons les connaissances suffisantes pour mesurer les risques dans chacune de vos actions sur internet. Ainsi vous pourrez éviter les sites à risque, faire en sorte que votre ordinateur soit véritablement protégé, faire de votre box une forteresse... ah non ! J'avais dit que çà n'était pas possible... Tout dépend du point de vue !

Fort Boyard ou la marelle ?

Le niveau de sécurité que vous devez rechercher dépend directement de la confidentialité que vous désirez avoir et de l'importance des documents que vous manipulez. A l'extrême limite, supposons que vous ne fassiez que surfer sur internet nonchalamment, vous pouvez vous abstenir complètement de sécuriser votre accès. Aucun document ne peut vous être volé puisque vous n'en avez pas. Ceci n'est pas tout à fait vrai non plus puisque accepter d'héberger un pirate sur son réseau est aussi se rendre coupable de délits pénaux si votre pirate utilise votre réseau pour accéder à des réseaux pédophiles par exemple. Plus couramment il utilisera votre réseau pour télécharger illégalement sur des réseaux peer-to-peer des fichiers de musique et de films. Cela vous rend exclusivement coupable de « défaut de sécurisation » depuis la loi Hadopi 2 adoptée par le Sénat le 21 septembre 2009.

Avant d'entrer plus dans les détails sur les manières de sécuriser votre réseau, c'est-à-dire votre box en particulier mais aussi vos ordinateurs et leurs utilisateurs, nous vous proposons deux petits tests sous forme de QCM qui vous aideront, l'un à tester vos connaissances et l'autre à tester la sécurité de votre réseau.

Repères :

Entre les sept couches de la classification OSI et les configurations plus ou moins habiles de l'utilisateur lambda, il existe une multitude de niveaux informatiques susceptibles d'abriter des failles de sécurité. Thème par thème, les différentes fiches pratiques Panoptinet vont vous apprendre à mieux appréhender votre système dans son ensemble, en fonction de vos besoins et du degré de sécurité que vous souhaitez appliquer. Elles vous enseigneront également quelles sont les conduites à risque à éviter.