15. Comment réagir pour faire progresser les démarches de sécurité sur Internet ?

Le mardi 15 juin 2004, nous a démontré que même les grands de l'Internet sont vulnérables. Le service de résolution de noms de domaine d'Akamai, utilisé notamment par Microsoft®, Yahoo®, Google® et Apple®, serait à l'origine du problème qui, selon l'*Internet Storm Center*, aurait probablement affecté le monde entier.

Pendant quelques heures, leurs sites ne fonctionnaient plus et au monde entier Internet n'était plus accessible pendant un certain temps ! Cette panne aurait été causée par un réseau d'ordinateurs infectés par des *chevaux de Troie* et commandés à distance pour lancer des attaques par déni de service.

Les responsables de ces attaques sont les internautes qui n'ont pas de protection antivirus, ni de firewall.

Pourquoi les internautes ?
Tout simplement parce que les ordinateurs infectés cachent des chevaux de Troie qui aident les malfaiteurs à employer leurs ordinateurs comme point de distribution du pourriel (spam) et de code malicieux.

Les internautes non protégés prêtent sans le savoir leurs ordinateurs comme station relais et ils s'interconnectent (de PC à PC) pour lancer des attaques renforcées. Nous sommes donc tous partiellement responsables de ces attaques virales si nous n'avons pas bien protégé notre ordinateur. http://www.webwizardbiz.com/tutorials/responsabilites

Comment réagir ?

Pour combattre ce fléau il suffit de respecter quelques règles. Le plus important est de faire les mises à jour (patches), les updates, de chez Microsoft® et des autres.
Voir aussi l'article à l'adresse suivante : Updates
http://www.webwizardbiz.com/tutorials/guidesecurite/page4.html

Actuellement il n'y a que 20 % des utilisateurs Windows® (selon une étude de Microsoft®) qui ont fait régulièrement ces mises à jour (updates). Les autres 80 % des internautes ne l'ont pas fait, parce qu'ils ne voient pas l'importance de le faire.

Si nous faisions tous ces mises à jour (updates) et si nous installions un antivirus et un firewall (pare-feu), les malfaiteurs n'auraient presque plus de chance de polluer Internet avec des malware.
http://www.homepages.lu/gust.mees/mausi/securite/malware

Comme on peut le constater, le maillon faible, c'est nous, les internautes et pas seulement Microsoft®. D'ailleurs, Linux® et aussi les Mac® ont des vulnérabilités. La seule différence réside dans la popularité ; c.-à-d. : Microsoft® est le système d'exploitation (OS) le plus répandu et pour ceci aussi le plus attaqué, sans rentrer dans les détails (monopole, jalousie, racisme, etc.) !

Récapitulatif :

Si tout le monde fait un petit effort, les malfaiteurs auront du mal à progresser et on arrêtera la plupart de leurs activités !

Que faire ?

- Faire régulièrement les updates de Microsoft®, du Mac® et aussi de Linux®.
- Télécharger quotidiennement les mises à jour de l'antivirus et du firewall ; ceci se fait automatiquement pour les versions payantes et pour la plupart des versions gratuites (freeware / gratuiciels) vous devez le faire manuellement.

Guide pratique de la sécurité : http://www.webwizardbiz.com/tutorials/guidesecurite/

Cadence de mises à jour :

Ceci est en principe tous les 2ème mardis d'un mois ; sauf correctifs urgents !

Remarque :

Faire les update, ne prend pas beaucoup de temps. C'est ainsi qu'on s'engage sans frais pour un avenir de l'internet intègre et libre.

MINISTÈRE DE L'ÉDUCATION NATIONALE
ET DE LA FORMATION PROFESSIONNELLE
Centre de technologie de l'éducation