Bref guide de survie informatique du béotien

Avertissement

Ces rappels sommaires de règles minimales d'hygiène informatique ne feront pas de leur lecteur un « *athénien* » mais un « *béotien* » néanmoins fréquentable.

Comprendre la notion de sécurité

La sécurité peut se résumer en 5 phases :

- prévenir le risque,
- détecter la menace,
- réagir à celle-ci,
- corriger et stopper la propagation de l'incident et
- éviter sa reproduction.

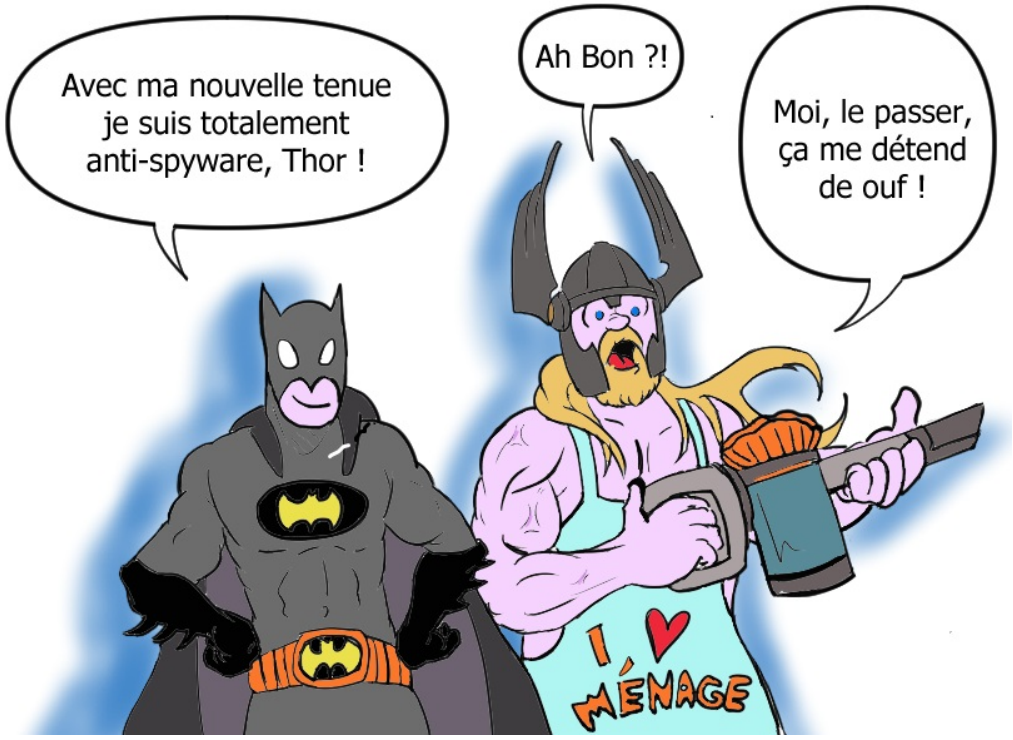
Maitriser le vocabulaire usuel des outils de protection

Le terme « *anti-malware* » prend peu à peu le pas sur le terme « *anti-virus* ».

Un malware est un logiciel malveillant qui ne se limite pas aux virus.

De plus ces logiciels n'ont pas tous la même finalité : la nature même du « *virus* » est d'assurer sa propagation, le « *spyware* » a pour vocation d'espionner, le « *rootkit* » confère à un tiers un accès frauduleux à la machine, le cheval de Troie est un logiciel qui abrite un programme illégitime.

A différents maux, différents remèdes et on parle alors d'« *anti-virus* », d'« *anti-spyware* » ou encore d'« *anti-rootkit* ». Ce sont tous des anti-malwares.



Pourquoi suis-je infecté ?

La réponse mérite sans doute un peu de tact mais la plupart du temps l'utilisateur participe activement à son propre malheur.

Par exemple si je ne clique pas sur le lien qui me permet de télécharger le fond d'écran de Pan-pan, le célèbre lapin de Disney, le fichier n'est pas exécuté et mon ordinateur n'est pas infecté.

Règle n° 1 : Si j'ai un doute, je ne clique pas

(traduction : si je ne connais pas le monsieur, je n'ouvre pas la porte).

De la même façon, quand je télécharge un logiciel gratuit (ou « *gratuiciel* ») sur une plate-forme de téléchargement, rien ne me garantit l'innocuité de ce logiciel.

Par défaut, il est mieux d'aller télécharger le programme sur le site de l'éditeur du logiciel.

Règle n° 2 : Je ne télécharge pas n'importe quoi n'importe où

(traduction : si je trouve un pain au chocolat qui est tombé par terre, je ne le mange pas).

Aussi, j'ai un ami spécialiste qui me dit que 80% des anti-virus ne marchent pas et qu'avoir un anti-virus ne protège que ma bonne conscience.

Mon ami est un athénien vous vous en doutez : moi, je mets toujours un anti-virus.

Règle n° 3 : Je mets toujours un anti-virus

(traduction : je suis déjà content qu'entre le monsieur et moi il y a une porte).

« Je ne comprends pas, ça marchait très bien avant la mise à jour (MAJ) … … d'ailleurs, je me demande si cela vaut vraiment la peine de les faire ! »

D'abord, tout utilisateur d'un ordinateur est une victime potentielle de la loi de Murphy : « *Tout ce qui est susceptible de mal tourner, tourne nécessairement mal* ».

Mais cette loi ne doit pas entraver votre propension à tendre vers le bien et donc à procéder aux MAJ.

Mettre à jour signifie mettre à jour le système d'exploitation et les logiciels figurant sur la machine.

Les MAJ permettent de parer aux failles de sécurité détectées.

Règle n° 4 : Je fais toujours les mises à jour du système d'exploitation et des logiciels

(traduction : je colmate la coque du bateau avant de prendre la mer même si je suis un bon nageur)

« Mon anti-virus est le meilleur du monde (c'est d'ailleurs marqué sur internet) il est à jour et pourtant il y a encore des trucs qui passent » (traduction : « *ma patience s'étiole* »).

Un anti-virus ne protège que des menaces qu'il connaît. La MAJ permet de collecter des signatures nouvelles de virus pour permettre à l'anti-virus d'accomplir sa tâche.

Mais le virus est parfois un mal impatient qui n'a pas toujours la décence d'attendre que l'anti-virus soit à jour.

Règle n° 5 : Chaque semaine, je fais un scan profond (celui qui dure longtemps) pour m'assurer que des malwares ne se sont pas installés avant la mise à jour

Rien n'interdit de faire autre chose pendant que s'opère le scan (il paraît que certains utilisateurs regardent fixement les fichiers scannés qui défilent voulant accéder à une vérité cachée qui se dérobe à eux).

Un ami athénien m'a dit qu'il faut *« compartimenter » »* (traduction : j'ai fait mine de comprendre pour garder la face).

Dans un premier temps, il convient de classer ses données (usuelles, importantes, capitales). C'est d'abord une affaire de sensibilité propre.

La question peut se poser ainsi : « *si je perds telles données, combien cela me coûte-il (en temps, en argent, en larmes, en regrets) ?* »

Investir dans un disque dur externe peut se révéler judicieux dans un certain nombre de situations : les données seront ainsi dupliquées et mises en sécurité (physique voire logique si chiffrement).

L'autre question à se poser est : « *si je perds tout, à qui vais-je m'en prendre* ? ».

Il est essentiel de configurer sur une machine au moins autant de sessions qu'il y a d'utilisateurs et de ne jamais travailler avec un compte administrateur :

- même si vous êtes le « *chef* » de l'ordinateur,
- sauf si vous êtes un athénien.

Pour les fichiers les plus sensibles, il existe des containers chiffrés plus largement décrits sur le site internet de l' Agence nationale de la sécurité des systèmes d'information (ANSSI).

Le réflexe santé

Aussi important que les 5 fruits et légumes par jour, il y a 5 principes élémentaires à observer pour l'utilisateur d'une machine :

- mettre des mots de passe,
- verrouiller la session utilisateur,
- empêcher le redémarrage par des périphériques externes (CD, clé USB),
- éteindre l'ordinateur s'il n'est pas utilisé,
- chiffrer le disque dur.

Règle n° 6 : 1234 et abcd ne sont pas des mots passe

Un mot de passe d'athénien :

- dispose de 12 caractères minimum avec des lettres, des chiffres et des caractères spéciaux,
- n'utilise pas de mots issus d'un dictionnaire,
- est parfois une phrase entière facile à mémoriser.

Quand il a peur de l'oublier, il ne le scotche pas sur son écran ou dans le tiroir de son bureau : il utilise des coffres forts numériques pour mot de passe permettant de stocker dans un seul et même fichier l'ensemble de ses mots de passe.

Et la boîte mail ?

Suivant certains historiens, Pandore avait une boîte mail …

Il faut savoir que 75% du trafic internet est constitué par des courriels et que 80% d'entre eux sont des spams (pourriels).

Aussi, la messagerie est un vecteur de propagation de l'insécurité numérique.

Bref rappel : un email est un fichier texte. Par conséquent, la pièce jointe (sauf à avoir la certitude de qui l'a envoyée) est un ennemi.

Aussi, si je clique sur la pièce jointe, j'exécute un fichier qui contient souvent un malware.

Règle n° 7 : Je ne clique pas si je n'ai pas de certitude

(traduction : si je veux un cadeau à l'intérieur je me rabats sur un kinder surprise).

Par ailleurs, je m'adonne à l'humour de bureau à temps perdu et j'envoie à mes collègues des liens vers des sites désopilants.

Tout d'abord, il faut lutter contre le côté noir de la force et ne pas céder aux sirènes de la lourdeur.

Ensuite (traduction : c'est déjà trop tard), il faut veiller à ne pas envoyer des images ou liens non vérifiés.

Enfin, l'envoi massif en copie carbone ou copie conforme « *cc* » est à éviter. En utilisant « *cci* » (« *bcc* »en anglais) copie carbone invisible, vous respectez la vie privée de vos contacts et luttez contre le spam.

« Je reviens d'un séminaire à Hong Kong, j'ai rapporté des goodies exceptionnels. »

Sinon à ce que leur dimension ornementale ne soit avérée, vous n'avez aucune raison valable de les conserver.

Quant à les enficher sur le port USB d'une machine (professionnelle ou personnelle) cela relève du sabotage.

Cela est valable tant pour la (super) clé USB 64Go que pour le chauffe-tasse ou le mini-ventilateur dont les couleurs criardes et le design incertain constituent déjà un appel à la prudence.

Règle n° 8 : Je ne branche rien sur un ordinateur qui ne soit vérifié ou de source fiable

Et le gagnant est ?

Nous avons tous un ami qui a un téléphone ou un ordinateur avec une pomme croquée.

Il vit avec la certitude que les malwares sont stoppés par le seul éclat de leur superbe machine.

Avec tout le tact que la situation nécessite, il est de votre rôle d'ami que de l'inviter à protéger ses équipements qui n'ont aucune raison d'être plus imperméables aux malwares que les autres.

Tous les systèmes d'exploitation ont des failles et tous sont des cibles potentielles. Ainsi l'hygiène informatique commande d'avoir la même vigilance quels que soient les équipements utilisés.

Pour finir, tout athénien a, dans le fond, une certaine forme de tendresse pour le béotien qui cherche à s'élever. Il ne faut donc pas hésiter à lui demander conseil.