Internet et la sécurité.

« Le moyen d'être sauf, c'est de ne pas se croire en sécurité » (Thomas Fuller)

Auteur : Alain Muller – almr13@free.fr

Table des matières

1. Objectifs de ce document.

Ce document n'est pas un tutorial. Il est destiné à sensibiliser le lecteur sur certains risques encourus en se connectant sur le cyberspace. Il n'a pas la prétention d'être exhaustif mais de donner un aperçu général tant du point de vue des risques que des moyens de les prévenir.

AVANT TOUTE CHOSE CE DOCUMENT EST UN DOCUMENT DE SENSIBILISATION.

2. La Loi

Déclaration universelle des droits de l'homme : article 12 :

> « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

Loi n° 78-17, article 1er :

> « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »

UN DROIT QU'ON NE PROTÈGE PAS, RISQUE D'ÊTRE PERDU

Code la propriété intellectuelle

Article L.335-3

> « Est (…) un délit de contrefaçon la violation de l'un des droits de l'auteur de logiciel […] »

Article L.122-4

> « Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur […] est illicite »

Article L.335-2

« La contrefaçon en France […] est punie de deux ans d'emprisonnement et de 15 000 € d'amende »

IL EST INTERDIT D'UTILISER DES LOGICIELS PIRATÉS, C'EST À DIRE ILLICITE.

Il est interdit de s'introduire dans un système d'information.

Le code pénal sanctionne différentes atteintes à la Sécurité des systèmes d'information :

–L'intrusion : l'article 323-1 dispose " Le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15.000 € d'amende "

–Le sabotage et les altérations : l'article 323-1 alinéa 2 dispose " Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30.000 € d'amende. "

IL EST INTERDIT DE S'INTRODUIRE DANS UN SYSTÈME D'INFORMATION MÊME SI CE DERNIER N'EST PAS PROTÉGÉ.

3. Pourquoi dois je me protéger, je n'ai rien à cacher.

Il faut sécuriser un ordinateur pour ne pas permettre à un pirate d'en prendre le contrôle (à l'insu de votre plein gré comme dirait un cycliste dopé) ou de s'en servir comme relais pour commettre un acte illégal. Ne pas protéger votre ordinateur c'est s'exposer au :

- ✔ vol de vos mots de passe
- ✔ L'usurpation d'identité
- ✔ Vol de vos fichiers
- ✔ vol du numéro de carte bleue
- ✔ A l'utilisation de votre ordinateur et de votre connexion internet pour faire des choses illégales comme spamer, envoyer des virus, diffuser illégalement des oeuvres protégés comme de la musique ou des films ou encore diffuser des images pédophiles. C'est techniquement possible et pas très compliqué, grâce au net qui

diffuse largement conseils techniques et logiciels, c'est même à la portée des néophytes.

Ne pas respecter les règles de sécurité, c'est vous exposer à des ennuis, qui peuvent aller de la simple gêne jusqu'à des poursuites judiciaires. Vous êtes **légalement responsable** de ce qui est fait à travers votre connexion internet. Sur le réseau, *vous n'êtes pas anonyme,* sinon comment pourrait-on vous faire parvenir les informations que vous demandez ? Votre fournisseur d'accès sait qui vous êtes et peut fournir votre identité aux autorités si nécessaire. Ce dernier est légalement tenu d'historiser vos connexions durant au minimum un an (voir 2 depuis la LEN, à vérifier). Les pirates peuvent utiliser votre ordinateur comme relais. Du point de vue de votre fournisseur d'accès internet, c'est *vous* qui aurez effectué ces actions, et c'est *vous* qui serez tenu pour responsable.

Ne pas sécuriser votre ordinateur, ça vous est préjudiciable, et c'est préjudiciable aux autres. Si un virus vous infecte, à votre insu vous infecterez d'autres machines à commencer par celles de vos contacts, des collègues, des amis, etc ...

Ne pas sécuriser votre ordinateur c'est s'exposer à des dysfonctionnements, certains logiciels malveillants comme les virus peuvent endommager votre système. Même après éradication du virus, votre système peut rester endommagé.

NE PAS PROTÉGER SON ORDINATEUR C'EST CONTRIBUER AU BORDEL AMBIANT ET MANQUER DE RESPECT POUR LES AUTRES.

4. Quelques chiffres.

Les quelques chiffres que je cite, je n'en sais malheureusement plus l'origine. Vous les prenez donc comme vous voulez. Cependant, une petite recherche sur internet vous permettra de vous rendre compte que si selon les sources et les périmètres étudiés (pays, professionnels de l'informatique ou pas, milieu social, etc ...) on trouve des variations significatives, ces chiffres se tiennent.

65 % du trafic français est lié au Peer to peer,

15 % du trafic internet est d'origine malveillante sans parler du spam.

25 minutes c'est le temps moyen de survie d'un PC sur le net sans protection.

Les dix virus les plus actifs en février 2005:

Les 10 virus les plus actifs en février 2005 selon F-Secure		
Rang	**Virus / Vers**	**% du nb total d'alertes**
1	Netsky.P	19,4%
2	Lovgate.W	12,3%
3	Netsky.Q	6,6%
4	Netsky.D	5,8%
5	Sober.K	3,7%
6	Zafi.D	3,6%
7	Bankfraud.CA	3,5%
8	Bagle.AT	2,8%
9	Netsky.B	2,3%
10	Bagle.Ay	2,3%

Tableau 1: Les virus les + actifs (tableau pris sur le journal du net et honteusement pompé sans même revoir la mise en forme)

73 % des internautes sont insuffisamment conscients des problèmes de sécurité.

DEUX CHIFFRES À METTRE FACE À FACE 65% ET 73% ...

QUELS SONT LES MENACES ?

1. L'escroquerie.

Hélas c'est courant sur internet en cherchant avec un moteur de recherche les mots « escroquerie » et « arnaque », vous tomberez sur un tas d'articles concernant les différentes pratiques. En voici quelques unes :

- ➔ Sollicitation de votre portefeuille par mail pour des prêts, des investissements, des aides financières, etc ...
  Ne jamais y répondre même par la négative.

- ➔ Achat en ligne jamais honoré mais la somme payée a été encaissée. Il s'agit d'une escroquerie à la fausse vente, cela arrive sur des sites marchands, des sites de ventes aux enchères etc ...
  Il faut porter plainte même si le site est étranger, si cela arrive sur une site de vente aux enchères le signaler aussi aux responsables du site. Vérifiez sur les forums, les sites d'association de consommateur, les annuaires whois que le site est connu et à pignon sur rue.

- ➔ Le phishing : le principe du phishing est d'obtenir, grâce à un e-mail factice (qui a l'apparence d'un courrier officiel envoyé par une banque, un cybermarchand ou un fournisseur d'accès internet), des données personnelles et bancaires d'un utilisateur. Sa participation repose sur sa crédulité, car c'est cet utilisateur qui fournit ces informations, en se rendant sur un faux site web, l'invitant à donner ses précieux sésames électroniques.
  Soyez prudents quand il s'agit de donner des informations personnels. Jamais par mail on ne donne un mot de passe même si il y a un formulaire fait pour. Vos fournisseurs d'accès n'ont aucune raison de vous les demander. Il ne faut jamais donner de numéro de carte bleue, ni de coordonnées bancaires sur un site non sécurisé et/ou non connu et/ou dont vous n'avez pas vérifié que le site est dûment enregistré et surtout *jamais après avoir cliqué sur un lien envoyé par mail. Ne jamais enregistrer dans vos favoris un lien envoyé par mail.*

- ➔ Les canulars ou hoax, certains sont inoffensifs et ne sont que des blagues de potaches. D'autres ont des buts néfastes et malveillants.
  Soyez vigilants, renseignez vous auprès de sites spécialisés, ne participez jamais à aucune chaîne, ne répondez pas aux mails d'inconnus ne les faites pas suivre, soyez réaliste la gratuité totale n'existe pas !

LE SEUL LOGICIEL VRAIMENT EFFICACE CONTRE LES ESCROQUERIES SUR LE NET, C'EST LE CERVEAU

2. Les virus et autres malwares.

Pour une liste plus complète et détaillée des différentes attaques je vous conseille de vous reporter sur le site http://assiste.free.fr/index.html sur le lien « attaques, contres mesures, liste de parasites ».

Lexique (non exhaustif) des malwares ou source.

Mots	***Définitions***
Adware	Logiciels destinés à vous bombarder avec de la publicité.
Backdoor	Littéralement porte par derrière, c'est une tâche destinés à maintenir un port ouvert sur votre machine. Dans un second temps cette tache permettra donc à quelqu'un connaissant la présence du backdoor d'accéder à votre système.
BHO	Browser helper object. Petit programme additionnel principalement pour internet explorer qui permet à des tiers d'ajouter des fonctionnalités au navigateur. Or ces ajouts ne sont pas toujours bienveillants ...
Malware	Terme générique définissant tous les programmes nuisibles ou parasites. Cela comprend, les virus, les spywares, les troyens, etc ...
RAT	Remote Admin Tool. Programme permettant de prendre le contrôle total d'une machine.
SPAM	L'encombrement délibéré d'un forum de discussion ou d'un compte mail par l'envoi de messages non sollicités, généralement des annonces à caractère publicitaire.
Spyware	Logiciel qui transmet des informations sur l'utilisateur ou sur ses habitudes généralement sans son autorisation et sans qu'il en soit conscient. Les destinataires sont généralement des annonceurs publicitaires. Cela peut-être aussi des éditeurs de logiciels qui espionnent les pratiques d'utilisateurs pour soit-disant mieux cerner leurs besoins et pouvoir apporter les améliorations utiles à leurs softs ...

Mots	*Définitions*
Trojan ou Cheval de troie	Programme malveillant qui se cache dans une application valide contenant en réalité une fonction illicite cachée. Ce programme contourne les mécanismes de sécurité du système informatique, ce qui permet la pénétration par effraction dans des fichiers pour les consulter, les modifier ou les détruire. Le cheval de Troie peut passer inaperçu pendant des mois puisqu'il se dissimule sous l'apparence d'un logiciel inoffensif, par exemple un jeu, ou un petit utilitaire.
Vers ou worm	Virus se propageant via un réseau, internet en particulier. Différentes techniques sont utilisées, un grand vecteur d'infection est bien sûr la messagerie.
Virus	Un programme dont la particularité est d'avoir la capacité à se reproduire. Généralement hostile (mais pas forcément), il est susceptible d'infecter vos fichiers (principalement les fichiers exécutables) en y insérant une copie de lui-même. Il peut en résulter des dysfonctionnements divers, effacement du disque dur, etc. Certains Virus savent se rendre invisible pour l'anti-virus, voir le désactivent carrément.
Virus d'application ou de macro	Les applications sont les programmes que nous utilisons tel que le traitement de texte, excel etc. Ces applications ont parfois la possibilités de programmer des Macros. Les virus d'application sont programmés dans ce langage Macro et sont exécutés lors du lancement de l'application.
Virus du secteur d'amorçage	Ce virus s'attaque au « Boot Sector » d'un disque, c'est-à-dire son premier secteur, celui qui lui sert à démarrer. Dans le cas du disque dur principal de l'ordinateur, il s'agit du premier secteur lu au démarrage de la machine. Un tel virus est ainsi chargé à chaque démarrage, et acquiert alors un contrôle complet de la machine. Ces virus sont parmi les plus difficiles à déceler. Ils sont en effet chargés en mémoire bien avant que l'utilisateur ou un logiciel (y compris un anti-virus) ne prenne le contrôle de l'ordinateur.

Mots	*Définitions*
Virus furtif	Très difficiles à détecter on les appelle ainsi car ces virus ont la capacité d'essayer de se camoufler pour être invisible aux traitements de détection des anti-virus. Pour ce faire deux techniques : - faire croire au système que certains secteurs du disques sont défectueux (ces secteurs ne sont donc plus utilisés par aucun programme, ni inspectés par l'anti-virus) et le virus se loge dans ces secteurs. - Modifier le système d'exploitation pour faire croire que les fichiers infectés sont sains. Cette technique est aussi capable de tromper un anti-virus.
Virus polymorphe	Ce type de virus modifie sa signature à chaque nouvelle infection. Quand on sait que la principale technique des anti-virus pour détecter un virus consiste a se référer à une base de signature, on comprend bien que ses virus sont difficiles à détecter.

SE PROTEGER EFFICACEMENT.

1. Peut-on se protéger à 100% ?

Une boutade dit : " Le seul ordinateur 100% protégé est un ordinateur éteint et encore je n'en suis pas sûr". Il ne faut pas rêver, il y aura toujours un petit malin pour inventer un système permettant de contourner les protections en place. En voiture la ceinture de sécurité ne sauve pas forcément la vie non plus. Est ce que pour autant qu'on ne la met pas ?

2. Est ce que ça coûte cher de se protéger ?

Non, on peut protéger un ordinateur *gratuitement*. La gratuité est possible grâce aux milieux associatifs ou aux éditeurs de logiciels de protection qui ont intérêt a ce qu'un maximum de monde utilise leur logiciel. Ils donnent donc accès gratuitement à certains logiciels dans l'espoir de vous voir acquérir des versions payantes plus complètes, mais aussi pour aider à rendre internet plus sûr.
En tout état de cause, cela coûtera toujours moins cher que de perdre des données sensibles, de se faire escroquer ou de devoir passer par un prestataire informatique pour réparer son système.

3. Le quintet gagnant

VOUS
+
WINDOWS UPDATES
+
ANTI-VIRUS
+
FIRE-WALL
+
ANTI-SPYWARE

4. La meilleure protection c'est vous.

Un ordinateur n'est pas une machine à laver ou un produit électro-ménager quelconque, contrairement à ce qu'on essaye de nous faire croire dans les rayons de supermarché. Un ordinateur c'est compliqué et même très compliqué, rien d'anormal quand on songe à la multiplicité des acteurs et à la richesse des possibilités d'utilisation. En aucun cas l'on peut espérer simplement le brancher et que sa fonctionne sans avoir à comprendre comment ça marche, sans s'occuper de ce qu'il contient, de ce qu'il exécute ... Mieux l'on comprend le mode de fonctionnement d'un PC, mieux l'on est a même de comprendre les risques et de les prévenir.

Quelques conseils :

- Connaître son système : une bonne approche msinfo32.exe (utilitaire Windows faisant la cartographie du système et des principaux paramètres)
- Tenir à jour le système avec windows updates
- Tenir à jour ses logiciels de sécurité (anti-virus, anti-spyware, fire-wall, ...)
- Ne jamais ouvrir un mail dont on ne connaît pas l'expéditeur
- Ne pas laisser le volet de pré visualisation de son client de messagerie actif, si le message est au format HTML, ce dernier peut contenir du code viral le simple fait de pré visualiser le contenu entraîne l'exécution de ce code.
- Scanner la machine régulièrement avec l'anti-virus, mais aussi avec un anti-virus en ligne.
- Ne pas rester connecté sur le net sans raisons, dès que vous n'en avez plus besoin déconnectez vous.
- Ne pas utiliser de logiciels piratés
- Ne pas télécharger à tort et à travers, avant d'installer un logiciel téléchargé il faut toujours scanner le ou les fichiers d'installation avec l'anti-virus et l'anti-spyware.
- Utiliser un autre navigateur qu'internet explorer (mon conseil : Firefox).
- Utiliser un autre client de messagerie qu'outlook express (mon conseil Thunderbird).
- Ne jamais accéder au net par un lien issu d'un message, ne jamais donner de renseignements personnels par ce biais, ni mot de passe, ni numéro de carte bleue.

- Soyez conscient que ni votre banque, ni votre fournisseur d'accès internet, ni Microsoft, ni qui que ce soit de sérieux n'a de raison de vous demander quels sont vos mots de passe.
- Ne pas répondre aux mails sollicitant quelque chose auprès de vous si vous ne connaissez pas l'expéditeur.
- Ne participez pas aux chaînes même si le prétexte est humanitaire ou généreux, je dirais même surtout dans ce cas là, le principe même d'une bonne escroquerie étant d'abuser de la générosité des gens.
- Ne laissez jamais votre adresse mail dans des forums ou des news-groups
- Ne jamais accédez au net sans que le fire-wall et l'anti-virus ne soient actifs
- Choisissez des mots passes difficiles à trouver, pas de nom d'enfant, du chien du chat ou de date de naissance. Un bon mot de passe fait au minimum 8 caractères contient des minuscules, des majuscules, des chiffres et si possibles même des caractères spéciaux (%;#,etc ...).

5. Windows Updates

- Lancez Internet Explorer
- Allez sur http://windowsupdate.microsoft.com
- Cliquez sur « *Rechercher des mises à jour* », et attendez un peu.
- Sélectionnez toutes les mises à jour critiques et cliquez sur « *Installer maintenant* ».(Il est possible que vous ayez à redémarrer votre ordinateur plusieurs fois à la suite de ceci.)
- Revenez sur http://windowsupdate.microsoft.com jusqu'à ce qu'il n'y ait plus de mise à jour critique à installer.
- C'est terminé !

6. Qu'est qu'un anti-virus

C'est un programme chargé de lutter contre les virus informatiques. Un anti-virus a deux méthodes principales pour protéger votre machine.

- Il se base sur une bibliothèque de signatures qu'il faut tenir a jour. Il lit vos fichiers et recherche si ces derniers ne contiennent pas une des signatures de sa bibliothèque en cas de correspondance, il sait que le fichier est infecté.
- Il utilise une méthode dite méthode heuristique, il s'agit d'un procédé d'intelligence artificiel, pour détecter des virus en les reconnaissant selon ce qu'ils sont capables de faire plutôt que selon une signature fixe.

En dehors de votre anti-virus local (celui que vous avez sur votre machine) il existe des anti-virus en ligne. Ces derniers ne peuvent en aucun cas remplacer l'anti-virus de votre ordinateur. Mais tous les anti-virus n'ayant pas exactement la même bibliothèque de virus, il peuvent être un bon complément. Voici quelques liens (attention, ils nécessitent la technologie ActiveX de Microsoft, donc en principe Internet Explorer) :

- http://www.secuser.com/antivirus/index.htm
- http://www.pandasoftware.com/activescan/
- Il y en a d'autres votre moteur de recherche préféré + les mots clefs "anti-virus en ligne" fera merveille, sans compter les liens que je vous donne dans ce document au paragraphe quelques sites internets utiles.

Attention : En général, quand vous achetez un ordinateur le constructeur vous fourni un anti-virus avec. La mise à jour de la base anti-virus (la bibliothèque de signatures) n'est gratuite que pendant un certain temps.
S'il vous faut un anti-virus, on en trouve des gratuits sur le net je vous suggère l'un de ces derniers :

- http://www.avast.com/
- http://www.grisoft.com/us/us_index.php
- Il y en a d'autres votre moteur de recherche préféré + les mots clefs "anti-virus gratuit" feront merveille.

7. Qu'est ce qu'un fire-wall ou Pare-feu ?

Dispositif (logiciel, serveur, ...) conçu pour protéger du piratage informatique un réseau ou un ordinateur connecté sur Internet. Ce dispositif permet d'assurer la sécurité en filtrant les entrées et en contrôlant les sorties selon une procédure automatique bien établie. En aucun ce n'est anti-virus. Le par-feu ne fait qu'agir que comme un garde barrière, il laisse entrer ou sortir l'information.

Windows XP à un pare-feu d'intégré il faut l'activer. Ce dernier ne filtre que ce qui entre et ne filtre rien sur le flux sortant. D'où les vives critiques que l'on peut rencontrer à son égard.

Vous trouverez sur ce site de plus amples renseignements sur les pare-feu : http://www.firewall-net.com/fr/

Il existe des pare-feu gratuit, personnellement je vous suggère Zone Alarm, vous le trouverez ici :http://www.zonelabs.com/

8. Qu'est ce qu'un anti-spyware .

Certains logiciels, contiennent un petit bout de programme qui va espionner ce que vous faites et l'envoyer à une entreprise sur internet qui le plus souvent revendra ces informations. C'est souvent le prix de la gratuité, je vous donne le logiciel et en échange j'épie vos faits et gestes sur le net. La transaction peut paraître honnête, seulement la plupart du temps elle est faite à votre insu et sans que vous puissiez contrôler, les informations épiées, inadmissible ! Même certains logiciel payant le font et certains grands éditeurs ne se gênent pas. C'est une atteinte à la vie privée ...

Pourquoi les antivirus ne les détectent pas ?

Techniquement, ce ne sont pas des virus puisqu'ils ne se reproduisent pas. Il est donc nécessaire d'installer un programme qui détecte spécifiquement les spywares.

Je vous en propose 2 qui sont gratuits et efficaces, je vous suggère même de prendre les deux, ils se complètent bien:

- Spybots S&D téléchargeable sur ce lien : http://www.safer-networking.org/fr/index.html (c'est gratuit et il est réputé comme étant un des meilleurs)
- Adaware de lavasoft téléchargeable sur ce lien : http://www.lavasoft.de/

9. Attention aux bons conseils y compris les miens ;-).

J'ai souvenir d'avoir conseillé Zone alarm à un ami, il a rencontré un problème de compatibilité avec son logiciels anti-virus, résultat plusieurs semaines sans protection réelle. C'est une anecdote ... mais avant d'installer quoique ce soit il faut lire la documentation, chercher sur le site de l'éditeur dans les FAQ (foire aux questions) ou dans les forums quels sont les problèmes que l'on risque de rencontré.

Certains logiciels de protection sont des spywares en puissance il faut le savoir, un des liens que je vous propose dans la liste des sites internet utiles possède une liste (sans doute non exhaustive) de ces faux utilitaires : http://assiste.free.fr/p/faux_utilitaires/faux_utilitaires_frameset.php

LES CONSEILLERS NE SONT PAS LES PAYEURS, SEULS VOUS POUVEZ DÉCIDER CE QUI EST BON POUR VOUS !

10.Quelques sites internet utiles.

Sites Internet	***Commentaires***
http://assiste.free.fr/index.html	Un Lien indispensable ! Vous saurez tout ce qu'il y a a savoir sur la sécurité accessible aux néophytes Des pages très intéressantes : Tester votre anti-virus, liste d'utilitaires, de spyware, liste de logiciels propres,etc ...
http://frenchmozilla.sourceforge.net/	Site ou vous pourrez un lien pour télécharger Firefox et/ou ThunderBird
http://securinet.free.fr/index.html	Un bon site généraliste pour comprendre les risques.
http://www.adresseip.com/	Un lien pour connaître son adresse IP
http://www.cnil.fr/index.php	Loi sur la tenue de fichier nominatif, mais aussi une mine de renseignements sur les traces que vous laissez et ce que l'on peut savoir d'un internaute depuis le net.
http://www.firewall-net.com/fr/	Sur ce site tout ce qu'il y a à savoir sur les fire-wall ainsi que des tutoriaux pour apprendre à les paramétrer.
http://www.generic-nic.net/dyn/whois/	Annuaire Whois pour tout connaître sur un site internet.
http://www.hoaxbuster.com	Pour vous aidez à déjouer les canulars
http://www.lesarnaques.com	Pour vous aidez à déjouer les arnaques et autres escroqueries
http://www.pandasoftware.com/activescan/	Antivirus en ligne de Panda Software
http://www.secuser.com/antivirus/index.htm	Anti-virus en ligne de House Call
http://www.secuser.com/index.htm	Un excellent portail très complet. Je vous conseille même de vous abonnez à la « news letter » de ce site.