annexe

C

Je le pris dans les bras. Je le bergai.
Je lui disais :
" La fleur que tu aimes
n'est pas en danger...
Je lui dessinerai une muselière
à ton mouton...
Je te dessinerai une armure
pour ta fleur..."

Le Petit Prince, A. de Saint Exupéry

Éléments de sécurité informatique

L'Internet d'aujourd'hui ressemble un peu au Far West du XIX^{e} siècle : il s'agit d'une terre de liberté et de grands espaces, une prairie sans barbelés, habitée par des peuplades et des cultures nouvelles... mais où pullulent les desperados ou les « docteurs » douteux vantant les mérites de leur antivirus à l'huile de serpent. Et les shérifs sont souvent débordés... Alors apprenons à nous débrouiller seuls, en attendant la cavalerie !

Sommaire

Contexte de cette annexe

Tout le monde a entendu parler de sécurité informatique – souvent à ses dépens. Quiconque a eu affaire un peu sérieusement avec l'Internet a en tête quelques idées sur les virus, les chevaux de Troie (*trojans*), les vers, voire les *root kits*, les crackers et les hackers... sans toujours vraiment savoir ce que c'est. Or, connaître le danger est la première étape qui permet de quitter le domaine de la peur et des incertitudes, et de prendre des mesures de défense appropriées.

> Technique **Un modèle de menaces pour le prix d'un livre !**
> La première étape dans une démarche de sécurisation d'un système informatique est de savoir ce qu'on risque et de la part de qui ou quoi – on appelle cela « établir un modèle de menaces ». C'est à cela même que nous nous attelons dans cette annexe pour le cas précis d'une messagerie et d'un site web associatifs, d'où le choix du plan – notons que ce service, lorsqu'il est rendu par un professionnel, et non dispensé dans un livre, coûte habituellement fort cher, étant donné que le client des officines de sécurité informatique a bien souvent littéralement le couteau sous la gorge ! D'un autre côté, le rapport est beaucoup plus épais, et souvent en couleur.

Il ne sera pas question ici des saloons malfamés de l'Internet (ce n'est pas de la sécurité informatique que d'apprendre à se tenir à l'écart de tels lieux...), ni de copie frauduleuse de fichiers MP3 (c'est là une question juridique, qui n'a rien à voir avec la sécurité informatique – voir le tableau C-1), ni de mercenaires sans pitié (le profil psychologique des « méchants », comme on le verra, est assez décevant). En revanche, nous verrons qui a intérêt à attaquer les serveurs ou le courrier électronique de l'association, et... qui peut se retrouver en train de le faire complètement par hasard ! Et évidemment, quoi faire pour s'en protéger.

Tableau C–1 Quelques mythes ayant trait à la sécurité informatique

On dit souvent que...	La vérité, c'est que...
La copie de DVD et l'intrusion sur des systèmes informatiques sont tous deux des actes de piratage. La sécurité informatique consiste à empêcher ces actes (DVD incopiables, par exemple).	Il n'existe pas plus de DVD incopiables (ou quoi que ce soit qui s'enregistre dans un ordinateur : images, sons, programmes...) que d'eau qui ne mouille pas. Cette confusion de langage va dans le sens de ce que les majors (maisons de disques, de DVD et Microsoft en tant que milice technique) aimeraient obtenir : imposer par le biais de la loi que tous les ordinateurs soient mutilés d'une partie de leurs fonctions naturelles de copie par le moyen d'une puce de supervision placée à l'intérieur et exécutant du code contrôlé par lesdites majors. La sécurité contre les intrusions est le cadet de leurs soucis (voir ci-après). Bruce Schneier, revue Crypto-Gram : **http://www.schneier.com/crypto-gram-0105.html** **http://www.schneier.com/crypto-gram-0110.html#3**
L'insécurité des ordinateurs est une fatalité : tout programme comporte des bogues car l'erreur (du programmeur) est humaine.	Ce n'est qu'une partie de la vérité : un couple homme-machine bien conçu doit permettre à la machine de parer certaines défaillances de l'homme. Il existe des systèmes d'exploitation (comme Linux ou les BSD !) prévus pour minimiser l'impact des erreurs de programmation ; on peut améliorer la culture de sécurité auprès des programmeurs (dont l'attitude est trop souvent « dès que ça marche, j'ai fini mon travail »), se contraindre à une relecture de tous les programmes critiques par des experts indépendants, mettre en place un programme de suivi et réparation des failles de sécurité chez les utilisateurs. Rien de tout cela ne se fait dans le monde des logiciels propriétaires, parce que la sécurité ne fait pas vendre... et que l'insécurité ne coûte rien (les éditeurs de logiciels ne sont pas légalement responsables des dégâts causés par les vices de conception de leur système, qu'ils aient trait à la sécurité informatique ou aux plantages inopinés). **http://security.tombom.co.uk/shatter.html** **http://www.openwall.com/Owl/fr/CONCEPTS.shtml** Roberto Di Cosmo, « Le hold-up planétaire » : **http://www.dicosmo.org/HoldUp/**

Tableau C–1 Quelques mythes ayant trait à la sécurité informatique (suite)

On dit souvent que...	La vérité, c'est que...
Les virus informatiques et les vers sont une évolution naturelle des programmes, similaires à leurs homologues biologiques. Ils sont inévitables au même titre que les bogues.	Ce sont des programmes délibérément écrits pour nuire et se propager d'ordinateur en ordinateur. Ils profitent de l'état déplorable de la sécurité informatique sur la plupart des systèmes d'exploitation commerciaux (voir ci-dessus) pour agir. Écrire un virus informatique fut autrefois un exercice très difficile, réservé aux plus brillants programmeurs ; certains le firent au début pour prouver de façon patente la criticité d'un bogue que les éditeurs refusaient de reconnaître (voir ci-dessus), la nuisibilité ne vint qu'ensuite. C'est devenu un jeu d'enfant avec l'avènement de l'Internet pour tous et de logiciels (traitements de texte, logiciels de courrier électronique, navigateurs...) mal conçus, qui exécutent toutes les instructions qu'on leur donne sans vérifier leur provenance ni leurs conséquences (un peu comme si on acceptait de manger un sandwich qu'un inconnu nous tend à brûle-pourpoint en pleine rue). **http://www.lacave.net/~jokeuse/usenet/faq-fcsv.html** **http://world.std.com/~franl/worm.html** Outil de création de « vers », en espagnol mais les captures d'écran sont éloquentes : **http://www.perantivirus.com/sosvirus/hackers/kalamar.htm**
Des logiciels (provenant parfois d'éditeurs célèbres) installent des espions qui renseignent via Internet leur fabricant sur la vie privée de l'utilisateur (numéro de version des autres logiciels installés, préférences en matière de visites de site web...).	C'est parfaitement exact. **http://edition.cnn.com/2002/WORLD/europe/06/17/eu.cookies/** **http://lists.essential.org/1995/info-policy-notes/msg00151.html** **http://www.spywareinfo.com/**

Tableau C–1 Quelques mythes ayant trait à la sécurité informatique (suite)

On dit souvent que...	La vérité, c'est que...
Les pirates informatiques qui attaquent les réseaux sont des idéalistes anarchistes cheveux au vent, des rebelles !	Ce sont le plus souvent des adolescents en mal de reconnaissance sociale sans aucune compétence, utilisant des outils d'attaque automatique écrits par d'autres. Ils s'estiment satisfaits lorsqu'ils ont défiguré un site web ou fermé un chat (dont ils sont à ce point friands pour combler leurs carences sociales qu'ils s'imaginent que c'est le cas pour tout le monde). **http://www.e-commercealert.com/article344.html**
Les « hackers » attaquent les ordinateurs pour en comprendre le fonctionnement, sans intention de nuire.	C'était vrai il y a 20 ans, quand chaque ordinateur coûtait des millions et que l'étudiant moyen n'y avait accès que par cartes perforées interposées. Aujourd'hui, les gens intéressés pour apprendre la sécurité informatique par l'expérience se procurent un PC sous Linux et aident à sa programmation... Les développeurs de Linux s'appellent toujours hackers (« bricoleurs ») entre eux, mais à présent ils sont de l'autre côté de la barrière : ce sont eux qui écrivent le code qui protège contre les intrusions ! **http://www.pryde-lands.com/catman/hackhist2.pdf**
Tel ou tel « petit génie » de l'informatique a réussi à s'introduire dans les ordinateurs du Pentagone.	Les ordinateurs sensibles de l'armée américaine ne sont pas reliés à l'Internet. Ceux qui sont attaqués sont des appâts, utilisés pour des motivations politiques (obtenir des budgets pour la Défense nationale). Douglas Thomas, *Sorting out the hacks and the hackers* : **http://www.ojr.org/ojr/ethics/1017969499.php**
Serge Humpich est un vrai pirate, un hors-la-loi qui a cassé le secret des Cartes Bleues pour voler un euro sur le compte de tout le monde et ainsi s'enrichir.	Le système de sécurité des Cartes Bleues semble fragile : le numéro de carte, par exemple, n'est rien d'autre qu'un login sans mot de passe. Le GIE Carte Bleue est sans doute conscient des problèmes. Que Serge Humpich soit désigné comme pirate, voilà qui évite une bien mauvaise publicité au GIE. Mais les vulnérabilités découvertes par Humpich sont toujours là... **http://www.parodie.com/humpich/**

Tableau C–1 Quelques mythes ayant trait à la sécurité informatique (suite)

On dit souvent que...	La vérité, c'est que...
Il faut à tout prix dissimuler les failles de sécurité des systèmes informatiques et interdire la diffusion sur l'Internet de programmes d'attaque.	La seule façon de contraindre un éditeur de logiciels à réparer les trous de ses programmes est de lui mettre le nez dessus. Pour un administrateur réseau, savoir s'il est vulnérable (en essayant l'outil d'attaque sur lui-même) est critique pour évaluer la balance des risques entre ne rien faire et interrompre le service pour réparation. De plus, la recherche active sur la sécurité (qui requiert des outils logiciels spéciaux, qui sont marginalement et par nécessité des outils d'attaque comme un tournevis l'est pour une serrure) est une nécessité pour améliorer la situation : si la compétence en la matière est rendue hors-la-loi, alors seuls les hors-la-loi auront cette compétence. Les « gentils » resteront dans l'incertitude... **http://www.schneier.com/crypto-gram-0111.html#1**
La cryptographie sert aux terroristes à communiquer sur Internet par le biais d'images pornographiques truquées.	Bien que ce soit techniquement possible, est-il raisonnable de crapahuter au fin fond de l'Afghanistan en trimbalant un ordinateur portable avec une pile à combustible de 25 kg (pour un mois d'autonomie en courant électrique) et un téléphone Iridium (aussi facilement repérable par un satellite espion que la diode du répondeur téléphonique en pleine nuit) ? L'Internet est certainement utilisé à mauvais escient, mais ce genre d'argument est surtout utile pour créer l'amalgame « cryptographie = terrorisme » dans le but inavoué de dériver vers « Je ne comprends pas pourquoi vous dissimulez vos e-mails. Auriez-vous quelque chose à cacher ? ». **http://www.transfert.net/a7413**

Sauvegardes !

Toute personne ou organisation qui envisage d'utiliser un ordinateur de façon sérieuse doit penser à la question des sauvegardes. Elles constituent la seule bouée de sauvetage fiable si, malgré tous les efforts de sécurité informatique déployés par l'association, une effraction informatique a lieu (voir plus loin la section Que faire en cas d'intrusion ?). La sauvegarde doit couvrir au minimum les données. Sauvegarder les programmes dans leur forme non installée (archive Zip, CD-Rom d'installation) est bien utile mais pas indispensable, à moins que l'association craigne de ne pas pouvoir les retrouver par la suite (cas d'un partagiciel rare, par exemple). Les sauvegardes de l'intégralité du système d'exploitation installé peuvent aider pour accélérer une restauration en cas de panne (disque dur flambé le plus souvent), mais sont coûteuses en place et elles n'aideront en rien pour la restauration après intrusion (toutefois, on pourra peut-être les utiliser pour savoir exactement à quelle date le pirate est entré).

Attaques aveugles

L'attaque la plus fréquente est celle perpétrée par un desperado isolé. Il s'agit très rarement d'un chasseur de prime ayant un contrat sur l'association, bien plus souvent d'un script kiddie, qui a choisi l'association comme cible... par hasard ! Son objectif est de compromettre les ressources informatiques (postes de bureautique et/ou serveurs) de n'importe qui, d'y placer un accès permanent (une « porte de derrière »), puis de détourner l'ordinateur ainsi piraté pour... en attaquer d'autres, afin d'accroître son cheptel, et ainsi de suite. L'apothéose de l'opération consiste à frimer avec ses copains sur IRC (« KeWl ! J'@i oWneZ 316 S3rVeRZ H1e !!#@!/ »), et/ou à lancer une attaque massive vers une cible que lui et son groupe de copirates détestent (le site de Nike, celui du Sénat américain, etc.).

Un cas particulier d'attaque de ce genre est celle lancée automatiquement par un ver ou un virus de courrier électronique. C'est l'étape suivante dans l'automatisation du piratage : l'auteur (beaucoup plus compétent qu'un simple kiddie) lance un programme qui sait attaquer tout seul d'autres cibles pour se propager et recommencer. La possibilité d'automatiser une

attaque sur les millions d'ordinateurs que comporte l'Internet vient du manque d'« infodiversité » des systèmes d'exploitation (Linux compris, d'ailleurs) : si une vulnérabilité existe sur un ordinateur, elle existe aussi sur des centaines de milliers de ses semblables. Une fois que l'attaque est lancée, elle échappe à tout contrôle ; le « but du jeu » pour l'auteur du ver est de mettre KO le maximum de réseaux en un minimum de temps et de faire les gros titres de la presse.

> **Script kiddie**
> Se dit d'un pirate en herbe techniquement inepte, et qui se borne à utiliser des outils (scripts) que ses ancêtres ont écrits pour lui (« cliquer-pirater » en quelque sorte). Grâce au téléchargement des logiciels *via* l'Internet, un seul ancêtre suffit pour des dizaines de milliers de kiddies, alors gageons que l'invasion ne s'arrêtera pas de sitôt... Il est courant d'essuyer en moyenne un « scan » tous les quarts d'heure (un « scan » est l'équivalent informatique d'un type louche qui essaie dans la rue d'ouvrir toutes les portières de voiture).

Contre-mesures

Pour repousser les kiddies, il suffit d'être un peu plus « sûr » que son voisin : celui-ci passera son chemin, à la recherche d'une proie moins protégée. Il faut établir des défenses périmétriques (installation d'un pare-feu) et en profondeur :

- Pour les ordinateurs de bureautique, un antivirus sur chaque poste, à maintenir à jour de façon bimensuelle (s'imprégner de la FAQ du groupe Usenet **fr.comp.securite.virus**, sise à **http://www.lacave.net/~jokeuse/usenet/faq-fcsv.html**).
- Pour les serveurs administrés par l'association, l'informaticien pratiquera une veille de sécurité hebdomadaire afin de mettre à jour tous les logiciels critiques du serveur (le noyau, Apache, BIND...) aussi souvent que nécessaire (consulter les sites **http://www.secuser.com/** et **http://perso.wanadoo.fr/websecurite/**).
- Pour les serveurs en hébergement partagé, on s'assurera auprès du fournisseur que lui-même effectue cette veille de sécurité.

- Choisir des mots de passe difficiles à deviner et en changer régulièrement, en suivant les recommandations de l'encadré Gestion et protection des mots de passe du chapitre 8.

> **Technique** **Installation d'un pare-feu**
> Un pare-feu est un dispositif de filtrage placé entre l'Internet et le ou les ordinateurs à protéger. Il fonctionne en interdisant certains protocoles suspects (IRC dans le cas où le serveur serait à l'intérieur du réseau de l'association, par exemple !).
> Le plus simple et le plus sûr, c'est de se procurer dans le commerce l'un de ces petits boîtiers qui permettent de partager une connexion Internet à plusieurs postes et qui proposent également un système de pare-feu configurable par un mini-serveur web à bord de l'appareil. L'informaticien du groupe s'en occupera, en partant d'une configuration paranoïde (à savoir : tout fermé sauf le Web et le courrier électronique sortant) et en assouplissant au fur et à mesure, plutôt que l'inverse.
> Consulter attentivement la notice de l'appareil, ainsi que **http://eservice.free.fr/pare-feu.html** et les autres liens de sécurité informatique cités ci-contre.

Attaques aveugles aggravées

Supposons qu'un desperado un peu plus compétent qu'un simple script kiddie ait visé un serveur, ait réussi à entrer, ait foré la « porte de derrière », et soit suffisamment au courant du système d'exploitation cible pour aller y faire un tour et faire main basse sur ce qu'il trouve. Ce peut être un fichier de mots de passe (auquel cas on peut aller jouer les trouble-fête sur un chat, rédiger et valider une page d'accueil « personnalisée » sur Spip, etc.)... ou, plus grave, comme des numéros de Carte Bleue.

Contre-mesures

Pour imaginer ce que pourrait faire un pirate en cas d'attaque aveugle aggravée, le plus simple est... de se mettre à sa place (c'est une gymnastique

d'esprit que pratiquent quotidiennement les professionnels de la sécurité – avec un peu d'entraînement, on arrive à rester sain d'esprit).

> Perspectives **Quid des vols de numéro de Carte Bleue ?**
> Si l'association met en place un moyen de paiement en ligne sur le serveur, opter pour un système dans lequel les informations de Carte Bleue ne transitent jamais par le serveur de l'association mais sont directement validées auprès de la banque.

Une attaque aggravée sur un poste client peut tourner à la catastrophe, parce que ses méandres sont probablement remplis de fichiers intéressants : numéro de Carte Bleue de l'association, fichier des membres avec mots de passe et adresses e-mail, etc. C'est une raison suffisante pour mettre en place une sécurité périmétrique en béton : le siège de l'association doit être protégé par un pare-feu de telle sorte qu'il soit invisible depuis l'Internet.

Reste la question des serveurs qui, dans la mesure du possible, ne doivent rien contenir de sensible, du moins rien qui puisse causer la compromission d'autres services informatiques. Si le serveur dispose d'une base de données de mots de passe, elle doit être chiffrée (d'où la manœuvre finale d'effacement des mots de passe en clair dans l'exemple du chapitre 8). Au moindre doute de compromission du serveur, changer les mots de passe de tous les utilisateurs après la réinstallation (voir plus loin la section Que faire en cas d'intrusion ?).

Attaques ciblées opportunistes

Il s'agit par exemple d'un logiciel web mal installé qui laisse voir son fichier de mots de passe (voir le chapitre 8). Dans ce cas, un individu compétent pourra se dire « tiens, tiens... » et, selon son humeur du moment, envoyer un e-mail d'avertissement à l'adresse « Contact », oublier l'affaire et passer son chemin, ou bien se mettre à exploiter la faille...

> **Perspectives** **Spammeurs et adresses électroniques**
> De façon périphérique à la sécurité informatique, se pose la question d'empêcher les spammeurs d'accéder à la base des adresses électroniques des utilisateurs du site. Pour cela, il faut vérifier que les moyens d'y accéder sont bien surveillés :
> - L'écran « Afficher la liste des abonnés » de l'interface de gestion en ligne de la liste (s'il y en a une) réclame bien un mot de passe.
> - Surveiller l'archive en ligne de la liste anonyme des adresses.

Contre-mesures

- Prêter une oreille attentive à ce que disent les visiteurs du site, même et surtout si c'est technique !
- À chaque fois qu'on crée un fichier comme `.htpasswd` ou `.htaccess` (comme décrit au chapitre 8), bien vérifier avec son navigateur qu'on ne peut pas le lire depuis le Web.
- Lire attentivement les documentations des logiciels installés sur le serveur, y compris la section « Sécurité » (on peut y revenir une fois que « ce qui est important » marche, mais ne pas oublier !).

Attaques ciblées motivées

C'est un cas rare, sauf pour une association qui a des ennemis déterminés et compétents (par exemple, une ONG ou une association d'activistes) : dans ce cas, un bras de fer va s'engager entre le pirate et l'équipe informatique de l'association. Les cibles classiques sont l'espionnage du courrier électronique (le système d'espionnage américain Echelon lit le courrier électronique de tout le monde en Europe par exemple – **http://www.unesco.org/webworld/infoethics_2/eng/papers/paper_12.htm**) et des mots de passe système lors de l'utilisation d'un protocole non sûr (comme le sont malheureusement FTP, HTTP et Telnet – utilisé pour l'accès au « shell », voir le chapitre 3).

> Perspectives **Bienvenue à Paranoïa...**
> Lorsqu'une association a des ennemis déterminés et compétents, la sécurité informatique telle que présentée ici n'est que la partie émergée de l'iceberg ! Quid des « taupes » qui s'inscrivent en tant que membre ou même permanent de l'association (il est tellement plus facile de réussir un piratage lorsqu'on dispose déjà d'un mot de passe, même restreint...) ? Quid du monte-en-l'air entrant nuitamment dans les locaux muni d'un ordinateur portable et d'un graveur de CD-Rom ? Et ce, bien sûr, sans compter les considérations de sécurité tout court : incendies causés par un militant aviné, pressions personnelles en tous genres sur les membres de l'association...

Contre-mesures

Le mieux que l'on puisse faire, c'est espérer avoir une longueur d'avance sur ses ennemis :

- Maintenir une veille de sécurité particulièrement consciencieuse (voir plus haut Attaques aveugles – contre-mesures).
- Pour les serveurs que l'association administre elle-même, installer un logiciel de détection d'intrusion tel que Snort (**http://www.snort.org/**) et un système de contrôle d'intégrité binaire tel que AIDE (**http://aide.sourceforge.net/**). Avec ce dernier, il faut effectuer un redémarrage contrôlé qui nécessite la présence physique d'un opérateur devant la machine – à faire au moins une fois tous les deux mois.
- Utiliser des logiciels de remplacement pour FTP, HTTP et Telnet : respectivement SCP, HTTP/S et SSH (voir **http://www.chiark.greenend.org.uk/~sgtatham/putty/**).
- Employer un système de chiffrement du courrier électronique tel que PGP (le plug-in PGP pour Thunderbird s'appelle Enigmail, **http://enigmail.mozdev.org/**). Attention, son utilisation correcte nécessite une solide formation de la part de tous les intéressés ! (**http://www.pgpi.org/links/www/pgp/fr/**)

Que faire en cas d'intrusion ?

Mieux vaut prévenir que guérir... mais parfois il faut guérir quand même. En cas d'intrusion soupçonnée ou avérée sur un ordinateur, voici la démarche à suivre : la procédure est identique pour tout type d'attaque (virus, ver, piratage « manuel »).

- Avant tout, limiter les dégâts ! Éteindre ou faire éteindre l'ordinateur (de préférence en appuyant sur le gros bouton rouge plutôt qu'avec la procédure « propre », afin de ne pas endommager les « morceaux » d'outils du pirate pour l'autopsie).
- Prévenir qui de droit, aller boire un café, faire le tour du pâté de maisons, se détendre. Le danger est écarté, la suite est une opération de chirurgie qu'il ne faut pas aborder en étant tendu comme une corde à piano : on risquerait de faire des erreurs (se tromper de direction de copie au moment de dupliquer le Zip de sauvegarde par exemple...).
- Essayer de contacter un expert pour pratiquer l'autopsie du serveur : transplantation de son disque dur dans une machine saine, récupération des données qui peuvent l'être, découverte de la faille par laquelle le pirate est entré.
- Si possible, se procurer un ordinateur vierge (ou un disque dur vierge, qu'on permute avec le disque dur infecté à l'aide d'un tournevis cruciforme et de la notice du serveur). L'ordinateur ou le disque dur infecté ne pourrra être réutilisé qu'après que son autopsie aura été faite, et que l'expert l'aura intégralement effacé à l'aide d'un outil approprié (s'il n'en connaît pas, changer d'expert).
- Réinstaller le système d'exploitation de l'ordinateur vierge ou virginisé, avec tous les correctifs de sécurité connus à ce jour (à partir des CD-Rom d'origine et/ou de « patches » téléchargés fraîchement de l'Internet – et non pas d'une sauvegarde !). Si c'est un serveur, réinstaller les applications web (Spip, ShoutChat, etc.) également à partir de leurs dernières versions connues (et non pas à partir d'une sauvegarde !). Si c'est un poste de bureautique, installer un antivirus à jour.
- Changer tous les mots de passe du système d'exploitation.
- Récupérer la sauvegarde la plus récente (si possible, celle faite par l'expert, qui contient toutes les données jusqu'à l'Apocalypse) et la protéger en écriture : basculer le taquet de protection de la disquette ou

de la bande magnétique, ou bien s'assurer qu'il s'agit d'un CD-R et non d'un CD-RW, ou bien (dans le cas d'un médium sans protection matérielle contre l'écriture, comme un Zip) en faire une copie sur une machine saine. Réinstaller les données à partir de cette sauvegarde. Si c'est un poste de bureautique, vérifier scrupuleusement avec l'aide de l'expert que, ce faisant, on ne contamine pas la machine à nouveau : ne restaurer aucun fichier `.exe` ou `.com` depuis la sauvegarde, passer tous les documents MS-Office et les archives de courrier électronique à l'antivirus avant de les ouvrir.

- Si l'antivirus signale que les données sauvegardées sont elles aussi corrompues, récupérer une sauvegarde plus ancienne, jusqu'à ce que l'on en trouve une qui ne soit pas contaminée. Si elle est introuvable, faire une exportation des fichiers corrompus les plus récents dans un format texte (sans virus) tel que HTML ou PNG, sauvegarder le résultat sur un autre support que celui utilisé précédemment et... recommencer la procédure de décontamination du début !
- En cas de doute sur la contamination (« Zut ! je crois que j'ai lancé Word par erreur... »), même remède : on repart de zéro...
- Si l'expert a réussi à trouver par où le pirate était entré, lui faire vérifier que la vulnérabilité a disparu après mise à jour du système d'exploitation et des applications.
- Changer tous les mots de passe de toutes les applications qui en utilisent.
- Remettre la machine de remplacement en route et en réseau.
- Si l'ordinateur compromis comportait des données sensibles (en dehors des mots de passe) et qu'on a des raisons de soupçonner qu'elles ont pu fuir (attaque aveugle sur un serveur, qui a pu être aggravée d'un vol par le pirate, ou attaque ciblée), prévenir qui de droit – en particulier, la police.

En résumé...

La sécurité informatique ne s'invente pas et est encore malheureusement entourée d'un certain halo shamanique – ce qui compte, en définitive, c'est de se former en permanence pour rester à niveau en la matière. C'est une tâche dont l'informaticien du groupe web devra avoir à cœur de s'acquitter de façon particulièrement consciencieuse – l'incurie des administrateurs est en effet pour beaucoup dans l'état actuel de la sécurité informatique de l'Internet. Pour ce qui est des postes clients, il n'y a guère de recette miracle : en attendant l'avènement des systèmes bureautiques sous Linux, il faut vivre avec leur manque de sécurité criant...