SECURITE INFORMATIQUE

DSI-DE

Table des matières

Chapitre 1

Qu'est-ce que la sécurité

La sécurité consiste :
- à assurer la disponibilité, l'intégrité, la confidentialité des données
- à ce qu'un logiciel soit conforme à ses spécifications
- à éviter les indisponibilités, incidents, erreurs, négligences et malveillances.

Elle vise tout le système d'information, et ce à tous les niveaux (réseau, systèmes, logiciels, plugins,...). Cela va de la mise en place d'un code d'accès à une salle serveurs au suivi de correctifs de logiciels.

Chapitre 2

Les bonnes pratiques

La sécurité du poste de travail commence d'abord par un certain nombre de bonnes « pratiques » d'utilisation. Cela vous permettra d'éviter la plupart des menaces.

2.1 La distinction des comptes

Les systèmes d'exploitation récents (Windows 2000, XP, Vista, Mac OS X,...) ou d'autres depuis l'origine (linux, Solaris,...) intègrent la distinction entre les types de comptes : utilisateur, utilisateur avec pouvoirs ou administrateur. Pour l'utilisation quotidienne (navigation internet, rédaction de rapports,...), il faut utiliser un compte utilisateur. Le compte administrateur est nécessaire uniquement pour certaines opérations de configuration du système, d'installation de logiciels ou de mises à jour. S'astreindre à ceci peut sembler contraignant, mais se révèle très utile en cas de problème : seul le compte utilisateur est compromis. D'autre part, à l'École des Ponts, chacun se voit attribuer un login et un mot de passe. Ces données sont personnelles et confidentielles. La personne les détenant en assume la responsabilité. Aussi, il est important de fermer votre session (Linux ou Windows) après avoir fini de travailler et avoir quitté la salle. Si vous vous absentez quelques instants, pensez à verouiller votre session !

2.2 La qualité des mots de passe

Des outils ou des méthodes (John the Ripper, brute force) permettent de deviner un mot de passe. De la qualité ou de la force de votre mot de passe dépendront la sécurité et la confidentialité de votre système et de vos données.
Un bon mot de passe a une longueur suffisante (8 caractères), et est contitué d'une alternance de chiffres, de lettres (minuscules et majuscules) et de caractères non alphanumériques (virgule, point d'exclamation,...). Une technique pour constituer un bon mot de passe facile à mémoriser consiste à écrire une phrase et utiliser le premier caractère de chaque mot et en conservant ou interposant des caractères de ponctuation.
Exemple : "Mon chien est le plus beau !" donne "McelpB !"

2.3 Intégrité des données

Afin de se prémunir de la perte de données, il est important d'en effectuer une sauvegarde régulière. Différents mécanismes existent : copie à un instant T sur un support différent : autre disque dur, cdrom, clé usb,... sauvegarde totale régulière à intervalles réguliers, sauvegarde incrémentale à intervalles réguliers (seules les différences sont sauvegardées, l'espace de sauvegarde nécessaire est moins important).

2.4 La logique

Tout comportement anormal de l'ordinateur doit alerter : la souris bouge toute seule, l'ordinateur a souvent du mal à démarrer, l'antivirus s'est désactivé,... Dans ce cas, si ce n'est pas déjà fait, pensez à sauvegarder les données et à inspecter votre ordinateur (antivirus, mises à jour de sécurité,...). Si vous contatez que l'antivirus est désactivé sur un poste de travail de l'école vous pouvez avertir l'informatique pédagogique afin d'éviter toute propagation éventuelle de virus sur le réseau.

2.5 Le confidentialité des données

De nombreux logiciels offrent des options de sécurité, notamment concernant la confidentialité. Par exemple, sur un navigateur Internet, il est possible de ne pas mémoriser l'historique de la navigation, de ne pas mémoriser les différents mots de passes saisis, les cookies,... Sur un ordinateur portable, il est possible de crypter une ou plusieurs partitions afin d'éviter la divulgation de données personnelles en cas de perte ou de vol.

2.6 Le choix et l'installation des logiciels

Lors du choix d'un logiciel, il est important de s'assurer qu'il rendra le service voulu et uniquement celui-ci. En effet, certains logiciels ajoutent d'autres logiciels espions. Si le logiciel est disponible en téléchargement, s'assurer que le site l'hébergeant est reconnu comme fiable. Certains sites fournissent une somme de contrôle MD5 permettant de vérifier l'intégrité du téléchargement.

MD5 (Message Digest 5) est une fonction de hachage cryptographique qui permet d'obtenir pour chaque message une empreinte numérique (en l'occurrence une séquence de 128 bits ou 32 caractères en notation hexadécimale) avec une probabilité très forte que, pour deux messages différents, leurs empreintes soient différentes.

2.7 Le choix des réponses

A certains moments, le système ou les logiciels peuvent poser des questions auxquelles porter une attention particulière peut éviter des problèmes par la suite. Par exemple, lors de l'installation d'un logiciel, l'installation personnalisée, lorsqu'elle est proposée peut permettre d'éviter d'installer des logiciels superflus ou dont le comportement peut être gênant (ex : barre d'outils google lors de l'installation d'acrobat reader).

2.8 Porter attention aux alertes système

Le système peut afficher des alertes dans des fenêtres surgissantes (« popup ») ; il est intéressant de les noter pour un diagnostic ultérieur. D'autre part, le système émet des rapports dans des fichiers journaux (journal système sous Windows, mécanisme syslog sous Linux,...). Le consulter de temps à autre permet de prévenir d'un éventuel problème (ex : disque dur ayant de manière récurrente des problèmes de lecture ou d'écriture).

2.9 Les mises à jour

La plupart des éditeurs de systèmes d'exploitation et de logiciels fournissent des mises à jours (automatiques ou non) de leurs produits (ex : Windows update, Office update, dépôt sécurité de Debian,...). Ces mises à jour peuvent être de différentes natures : ajout ou modification de fonctionnalités et correction de failles de sécurité ou de bugs. Les ajouts ou modifications de fonctionnalités sont à tester et peuvent apporter d'autres failles. Il faut les exploiter avec parcimonie. Les correctifs de sécurité peuvent aussi apporter d'autres problèmes mais sont en général censés en corriger ! Les installer permet de rendre moins vulnérable votre ordinateur. Si celles-ci ne sont pas installées, il sera possible d'exloiter la faille par ce que l'on appelle un « exploit » disponible sur le web ou qu'un pirate aura programmé lui-même.

2.10 Le choix de la diversité

Certains systèmes d'exploitation ou logiciels sont sujets à plus d'attaques compte-tenu de leur forte implantation. Le recours à des systèmes ou logiciels alternatifs permet de limiter les risques. De plus, de nombreux logiciels sont gratuits, tout en offrant les mêmes fonctionnalités que certains commerciaux. Ils vous permettront de rester dans la légalité sans renoncer à la puissance de certains outils (ex : scilab, gimp, openoffice, firefox, linux correspondant respectivement à matlab, photoshop, microsoft office, internet explorer et windows).

2.11 Pouvoir faire marche arrière

Lors d'une modification importante du système, vous pouvez en effectuer une sauvegarde afin de pouvoir revenir à une situation stable en cas de problème. Sous Windows, il est possible de positionner un point de restauration. Ainsi, on peut désinstaller un logiciel qui n'a pas de procédure ou une mauvaise procédure de désinstallation.

L'attention portée au comportement de votre système d'exploitation et la pratique de quelques règles permettent d'éviter la plupart des problèmes et d'assurer une plus longue longévité à votre système.

Chapitre 3

Les différentes menaces

le but : amusement, gêner, accéder aux données

3.1 Les virus

« Un virus informatique est un programme informatique écrit dans le but de se dupliquer sur d'autres ordinateurs. Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, mais aussi les disquettes, les cédéroms, les clefs USB, etc.

Son appellation provient d'une analogie avec le virus biologique puisqu'il présente des similitudes dans sa manière de se propager et de se reproduire. On attribue le terme de « virus informatique » à l'informaticien et spécialiste en biologie moléculaire Leonard Adleman (Fred Cohen, Experiments with Computer Viruses, 1984).

Le nombre total de virus couverts par Sophos s'élevait à 93 875 (tous types confondus, en août 2004) d'après Mag-securs. Ce chiffre n'est qu'une approximation grossière du nombre réel de virus en circulation, chaque éditeur d'antivirus ayant intérêt à « gonfler » la réalité, d'autant plus que très peu de virus identifiés atteignent le stade de la diffusion massive sur les réseaux. La très grande majorité touche la plate-forme Windows. Le reste est essentiellement destiné à des systèmes d'exploitation qui ne sont plus distribués depuis quelques années, comme les 27 virus - aucun n'étant dangereux - frappant Mac OS 9 et ses prédécesseurs (recensés par John Norstad, auteur de l'antivirus Disinfectant).

Les virus font souvent l'objet de fausses alertes que la rumeur propage, encombrant les messageries. Certaines d'entre elles, jouant sur l'ignorance en informatique des utilisateurs, leur font parfois détruire des éléments de système d'exploitation totalement sains. »[1]

Sur le site de Symantec par exemple (http ://www.symantec.com/enterprise/security_response/), vous pouvez consulter la liste des virus, leurs effets, les détails techniques et éventuellement télécharger un correctif après infection.

Exemple de description pour le virus W32.Vispat.B@mm (les informations sont en Anglais) :

SUMMARY :

[1] Wikipedia http ://www.wikipedia.fr

```
Discovered: August 1, 2007
Updated: August 2, 2007 7:29:06 AM
Type: Worm
Infection Length: 69,664 bytes
Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me,Windows NT,
Windows Server 2003, Windows Vista, Windows XP

W32.Vispat.B@mm is a mass-mailing worm that gathers email addresses from
the compromised computer. It also changes the Start Page for Internet
Explorer and lowers Internet security settings.

Protection

    * Initial Rapid Release version August 1, 2007 revision 053
    * Latest Rapid Release version August 1, 2007 revision 053
    * Initial Daily Certified version August 2, 2007 revision 003
    * Latest Daily Certified version August 2, 2007 revision 003
    * Initial Weekly Certified release date August 8, 2007

Click here for a more detailed description of Rapid Release and Daily Certified virus
Threat Assessment
Wild

    * Wild Level: Medium
    * Number of Infections: 0 - 49
    * Number of Sites: 0 - 2
    * Geographical Distribution: Low
    * Threat Containment: Easy
    * Removal: Easy

Damage

    * Damage Level: Medium
    * Payload: changes the Start Page for Internet Explorer and lowers Internet secur
    * Compromises Security Settings: Lowers Internet security settings.

Distribution

    * Distribution Level: High
    * Subject of Email: Re:Ho sbagliato email
    * Name of Attachment: fotoamore.zip

Writeup By: Asuka Yamamoto
```

D'autres informations intéressantes sont communiquées (détails techniques, instructions pour supprimer manuellement le virus).

3.2 Les vers

« Un ver informatique est un logiciel malveillant qui se reproduit sur des ordinateurs à l'aide d'un réseau informatique comme l'Internet.

Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources afin d'assurer sa reproduction. La définition d'un ver s'arrête à la manière dont il se propage de machine en machine, mais le véritable but de tels programmes peut aller au delà du simple fait de se reproduire : espionner, offrir un point d'accès caché (porte dérobée), détruire des données, faire des dégâts, envoi de multiples requêtes vers un site internet dans le but de le saturer, etc. Les effets secondaires peuvent être aussi un ralentissement de la machine infectée, ralentissement du réseau, plantage de services ou du système, etc.

Des vers écrits sous forme de script peuvent être intégrés dans un courriel ou sur une page HTML sur internet. Ils sont activés par les actions de l'utilisateur qui croit accéder à des informations lui étant destinées.

Un ver peut tout aussi bien être programmé en C, C++, Delphi, assembleur, etc. Il utilise la plupart du temps des bugs de logiciels pour se propager. »[1]
Afin de vous prémunir contre ce type de risque, évitez d'activer les macros lorsque vous ouvrez un document dont vous ne connaissez pas le contenu ou l'auteur.

3.3 Les bombes logiques

« Une bombe logique désigne, en sécurité informatique, dans un virus, un cheval de Troie ou dans tout autre type de programme malveillant, les fonctions destinées à causer des dommages dans l'ordinateur cible. La bombe logique est donc la charge utile du programme, on l'oppose donc aux fonctions destinées à la réplication du code ou à sa diffusion.

On appelle une bombe logique un dispositif programmé dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système. »[1]

3.4 Le cheval de Troie

« Un cheval de Troie (trojan en anglais) est un type de logiciel malveillant, c'est-à-dire un logiciel d'apparence légitime, mais conçu pour subrepticement exécuter des actions nuisibles à l'utilisateur ; un cheval de Troie, dans un programme, tente d'utiliser les droits appartenant à son environnement d'appel pour détourner, diffuser ou détruire des informations. Le partage des programmes introduit la problématique des chevaux de Troie. Les trojans auraient été créés dans les années 80, par un jeune hacker allemand du nom de Karl Koch. »[1]

[1]Wikipedia http ://www.wikipedia.fr

3.5 Les macro virus

« Les macrovirus utilisent le langage de programmation d'un logiciel pour en altérer le fonctionnement.

Ils sont en pleine expansion, du fait qu'ils s'intègrent à des fichiers très échangés et que leur programmation est à portée de tous.

C'est Visual Basic qui permet d'écrire ces macro-commandes pour Microsoft Word et Microsoft Excel.

Le logiciel OpenOffice.org est potentiellement vulnérable à ce type de virus car il permet également la création de macros. Mais le logiciel n'exécute les macros contenues dans un document qu'après la confirmation de l'utilisateur, empêchant l'exécution du virus. Le 30 mai 2006, un « proof-of-concept » nommé Virus.StarOffice.Stardust.a par Kaspersky a été découvert, il n'est pas considéré par le groupe responsable de la suite bureautique comme un véritable virus.

Ces macrovirus s'attaquent principalement aux fichiers des utilisateurs. »[1]

3.6 Usurpation : de site, de mail,...

L'usurpation d'identité par le mail est très fréquente et aisée à réaliser. Il faut donc se méfier lorsque l'on reçoit un mail d'une personne connnue et dont le contenu étonne. Dans ce cas, ce n'est pas la peine de répondre à ce mail et d'utiliser un autre moyen de communication pour s'assurer de sa véracité ! Bien entendu, il ne faut pas le faire ; si nous parvenons à détecter l'auteur, son compte sera désactivé. L'utilisation de signature GPG permet d'authentifier l'expéditeur d'un mail. D'autre part, le chiffrement GPG permet de rendre illisible un mail par quelqu'un d'autre que son destinataire.
L'usurpation de site web se répand aussi, c'est ce que l'on appelle le « phishing ». Cette pratique a pour but de récupérer vos identifiants et mots de passe pour un site bancaire par exemple. En général, un mail vous propose de vous connecter sur le site de votre banque. L'adresse n'est pas exactement la même et vous êtes redirigés vers autre site. Il est préférable de se connecter sur ces sites par une recherche sur un moteur de recherche ou par saisie directe de l'adresse communiquée par l'établissement, puis d'enregistrer un signet/favori pour ce site.

Exemple de phishing : « Une fois n'est pas coutume, une autre banque est victime de phishing. Cette fois-ci, c'est la banque BNP Paribas et ses clients qui sont les cibles d'une nouvelle attaque par Phishing. Plusieurs internautes ont d'ailleurs déjà reçu un email aux couleurs de la banque qui demande au destinataire du mail de mettre à jour ses coordonnées bancaires en cliquant sur le lien intégré à ce même courrier électronique.

[1] Wikipedia http ://www.wikipedia.fr

Bien entendu, le lien en question renvoit l'internaute sur un « faux site BNP », très bien conçu qui demande à l'internaute de saisir ses coordonnées bancaires. Le site frauduleux est associé à l'adresse « secure.bnpparibas.net.banque ». Bonne nouvelle, l'extension Google Safe Browsing (voir la brève L'anti-phishing de Google bientôt dans Firefox) détecte bien ce site malveillant.

Pour en savoir plus sur le phishing, n'hésitez pas à consulter et à faire circuler notre dossier Dossier sécurité : Spam et Phishing. »[2]
De nombreux SPAMS incitent aussi à aller sur un faux site Ebay pour récupérer vos identifiants et mots de passe.
Dans les dernières mises à jour Windows XP, un plugin Internet Explorer réalise des tests anti-hameçonnage.

3.7 Les hoax

« En informatique, les canulars (appelés hoax en anglais) se trouvent souvent sous la forme de courriel ou de simple lettre-chaîne. Dans ce dernier cas, internet ne fait qu'amplifier un phénomène qui existait déjà à travers le courrier traditionnel.

A la différence des pourriels qui sont la plupart du temps envoyés de manière automatisée à une liste de destinataires, les canulars sont, eux, relayés manuellement par des personnes de bonne foi.

Les canulars sont souvent bâtis sur les mêmes modèles que les légendes urbaines. Dans ce cas ils en exploitent les caractéristiques de diffusion par colportage, ce qui renforce à la fois leur impact et leur audience.

- Messages alarmistes, ils peuvent contenir des instructions pour un second e-mail, annoncé comme contenant un virus « Hautement destructeur » (Exemple : « Attention, ce virus détruit toutes les données du disque dur », ou encore « Virus certifié par McAfee et Microsoft comme étant le plus destructeur jamais créé », « Faites l'action X, Y afin de l'éviter ») ; Or un second mail n'arrive pas nécessairement, ceci peut éventuellement décrédibiliser les véritables messages de prévention de ses contacts. Le hoax répond cependant à un certain nombre de caractéristiques, alarmistes en particulier (exemple de hoax sur le site du logiciel anti-virus McAfee).
- les fausses alertes aux virus qui circulent par courriel sont destinées à faire paniquer les utilisateurs novices, parfois à leur faire commettre des manipulations dangereuses

[2]http ://www.clubic.com/actualite-33011-nouvelle-attaque-de-phishing-pour-bnp-paribas.html

de leur système informatique et souvent à congestionner le réseau par leur diffusion hors de tout contrôle.
- des quantités d'adresses e-mail sont aussi exposées, car souvent les utilisateurs ne savent pas les mettre en mode invisible ;
- on essaie de vous prendre par les sentiments de manière assez grossière (sauvez Brian !) ;
- les faits relatés sont généralement très flous (au Brésil, par exemple, sans plus de détail, ou dans 3 mois, sans donner la date de départ) ;
- les références sont généralement inexistantes ou au contraire trop énormes (le Pentagone, Microsoft, ...) ;
- parfois, on vous fait des promesses disproportionnées (devenir milliardaire vite et aisément, gagner un bateau, ...) ;
- parfois on vous assure à maintes reprises que ce n'est pas un canular, parfois en disant qu'un de ses amis a été convaincu par le message alors que c'est -évidemment- totalement faux ;
- on vous demande de renvoyer le message à toutes vos connaissances, ou à une adresse de courrier électronique bien précise
- enfin une variante appelée le viroax associe le virus et le hoax. Elle profite de la crédulité du destinataire, le pousse à effacer un fichier de son ordinateur, en lui faisant penser que c'est un virus, fichier parfois utile au fonctionnement de son système d'exploitation, son antivirus ou son pare-feu.

Parfois, et malheureusement, le message de départ est envoyé en toute bonne foi (vente de chiots, disparition de personne, demande de don de moelle osseuse...) mais il est ensuite expédié et ré-expédié par tant de personnes (voire -et très souvent- modifié) qu'il peut durer des années après la résolution du problème (qui a en général été réglé dans les plus brefs délais). On assiste alors à la diffusion massive de coordonnées personnelles de personnes dépassées par les évènements qui sont donc obligées de fermer leur adresse email, leur numéro de téléphone... pour retrouver la paix. Des associations, organismes ou hôpitaux ont étés victimes de ces débordements (par exemple l'American Cancer Society). »[1]
En cas de doute, le site http ://www.hoaxbuster.com/ référence un certain nombre de hoax et vous permettra d'éviter de recevoir un lien vers ce même site de la part de vos interlocuteurs relevant votre naïveté !

3.8 Le spam

« Le pourriel ou spam en anglais, désigne les communications électroniques massives, notamment de courriers électroniques, non sollicitées par les destinataires, à des fins publicitaires ou malhonnêtes... »[1] A l'École des Ponts, les boîtes à lettres de chacun sont protégées par un mécanisme de listes grises (greylists). Ce mécanisme consiste dans un premier temps à refuser temporairement un mail, puis à l'accepter ensuite. En effet, de nombreux systèmes d'envoi de spam ne gèrent pas les « erreurs temporaires » des mails et ne cherchent pas à le réexpédier plus tard, le but étant d'« innonder » le plus rapidemment possible le plus de boîtes.

[1] Wikipedia http ://www.wikipedia.fr

3.9 Les spyware

« Un logiciel espion (espiogiciel, mouchard ou en anglais spyware) est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur n'en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet, qui lui sert de moyen de transmission de données. »[1]

Chapitre 4

Se protéger

Différentes mesures de protection permettent de se protéger contre certaines menaces. Ces protections peuvent être mises en oeuvre sur des serveurs centraux (serveurs de votre fournisseur d'accès, serveurs de l'école) ou sur votre poste de travail, la combinaison des deux étant possible.

4.1 Pare-feu

Le pare-feu (ou firewall) limite l'accès en entrée et en sortie du réseau. Seules les fonctionnalités nécessaires et connues sont « ouvertes » (ex : messagerie : POP, IMAP, SMTP, pages Web : HTTP). Par exemple, l'accès aux pages web sur Internet correspondant au protocole HTTP (port 80) est ouvert en sortie. La plupart des réseaux sont équipés de pare-feu. Il est possible et conseillé d'en installer un sur son poste de travail (pare feu microsoft founi en standard à partir de Windows XP SP2, iptables sous linux,...).

4.2 Proxy

« Un serveur mandataire ou proxy (de l'anglais) est un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Les serveurs mandataires sont notamment utilisés pour assurer les fonctions suivantes :

- mémoire cache ;
- la journalisation des requêtes (« logging ») ;
- la sécurité du réseau local ;
- le filtrage et l'anonymat.

L'utilité des serveurs mandataires est importante, notamment dans le cadre de la sécurisation des systèmes d'information. Squid est le serveur opensource le plus utilisé. »

4.3 Antivirus

L'antivirus peut être installé à plusieurs niveaux : sur des serveurs de fichiers, sur le poste de travail ou sur une passerelle de mails. Sans mises à jour, son efficacité est quasiment nulle. Il faut veiller à ce qu'il soit actif en permanence afin de détecter un

virus dès l'ouverture d'un fichier. En général, une icône indique l'état de l'antivirus. A l'École des Ponts, l'antivirus MC Afee VSCAN est installé sur les postes Windows.

4.4 anti-spyware

4.5 Anti-spam

Différents mécanismes existent : filtres bayésiens, listes noires, listes grises, filtres avec reconnaissance de caractères pour les spam images.

« Le filtrage bayésien du pourriel (en référence à Thomas Bayes), est une technique de détection du pourriel utilisant les réseaux bayésiens et permettant le filtrage du courrier électronique. Le filtrage bayésien fut proposé par Sahami et al. en 1998 mais fut reconnu en 2002 lorsqu'il fut décrit dans un article de Paul Graham. C'est ensuite devenu une méthode populaire pour départager le courrier indésirable (spam) du courrier légitime (ham). Certains agents de courriers électronique modernes mettent en œuvre des filtres bayésiens antipourriels, et il est généralement possible à l'utilisateur d'installer des logiciels tiers spécialisés dans ce travail. Il est également possible de déployer ce type de filtres sur les serveurs à l'aide de logiciels spécialisés (comme SpamAssassin, SpamBayes, Bogofilter ou encore ASSP) ou lorsque le logiciel serveur supporte nativement cette fonctionnalité. L'empoisonnement bayésien (bayesian poisoning) est une technique utilisée par les polluposteurs pour tenter de dégrader l'efficacité des filtres antipourriels bayésiens. Elle consiste à inclure dans le courrier une grande quantité de texte anodin (provenant de site d'actualités ou de la littérature par exemple) pour noyer le texte indésirable et tromper le filtre.

Explication mathématique :

Les filtres antipourriels bayésiens reposent sur le théorème de Bayes. Le théorème de Bayes appliqué aux pourriels indique que la probabilité qu'un courrier soit un pourriel, compte tenu qu'il contienne certains mots, est égale à la probabilité de trouver ces mots dans un pourriel multipliée par la probabilité qu'un courrier soit un pourriel, divisé par la probabilité de trouver ces mots dans un courrier :

$\Pr(\text{pourriel}|\text{mots}) = \frac{\Pr(\text{mots}|\text{pourriel})\Pr(\text{pourriel})}{\Pr(\text{mots})}$ »

Le principe d'une liste noire est d'interroger une base ayant une liste de serveurs à bannir. Il peut arriver qu'un serveur légitime soit banni pour cause de mauvaise configuration. Le mécanisme de listes grises (greylinsting) est mis en œuvre à l'École des Ponts. Le principe est de rejeter temporairement un message. Si le serveur qui envoie ce dernier effectue une nouvelle tentavive, contrairement à la plupart des serveurs envoyant des pourriels, le message est alors accepté.

4.6 Les mises à jour de sécurité de l'os et des softs

cf. §1.8

Chapitre 5

En cas d'intrusion, d'infection ou de compromission

Lorsque le système est compromis, il est souvent trop tard pour rétablir l'ordinateur dans un état stable, une réinstallation du système d'exploitation, des logiciels et des données est nécessaire. L'analyse des journaux systèmes et l'utilisation de logiciels spécifiques peuvent permettre de diagnostiquer la nature de l'attaque. Les éditeurs d'antivirus préconisent des correctifs pour certains virus à posteriori sans avoir à réinstaller le système.

En cas d'intrusion, il y a souvent des « traces » permettant éventuellement de repérer l'auteur et/ou son activité sur l'ordinateur. Néanmoins, selon ses compétences, il tentera de masquer son passage. Ce dernier peut aussi chercher les votres : cache du navigateur web, mots de passe web. Les logiciels de navigation récents permettent d'effacer les « traces » .

cf : http ://www.cnil.fr/index.php ?id=123 !

Chapitre 6

Quelques règles à respecter

6.1 Licenses de logiciels

L'utilisation de la plupart des logiciels est soumise à une license d'utilisation. Il en existe de nombreux types offrant plus ou moins de droits (GPL,...).
Pourquoi prendre le risque juridique d'utiliser un logiciel de contrefaçon (dit aussi piratage) alors qu'il y a de très bons logiciels libres qui rendent les mêmes fonctionnalités ?

6.2 Netiquette

La netiquette est un code de bonne conduite sur Internet. Par exemple, on évitera de polluer une liste de diffusion avec des mails qui ne seraient pas en rapport avec celle-ci.

6.3 Téléchargement et diffusion de contenus illégaux

Certains téléchargements sont connus pour être illégaux en raison de la nature des données (musique et films soumis au droit d'auteur). A l'École des Ponts, vous avez la possibilité d'accéder à de nombreuses ressources documentaires en ligne. L'accès doit être limité à un usage normal : il est interdit d'essayer de télécharger le contenu total d'une ressource en ligne. Inversement, il est interdit de diffuser des contenus illégaux, par le biais de vos pages personnelles sur le serveur des élèves par exemple. Si tel était le cas, votre compte serait désactivé 3 mois.

6.4 Chartre informatique

La plupart des établissements demande à ses utilisateurs d'accepter une chartre informatique décrivant la bonne utilisation des ressources numériques. C'est le cas à l'École des Ponts.

6.5 Droit Français

Que l'établissement ait ou non défini une chartre informatique, chacun reste soumis au droit français dont certains articles font référence à l'informatique.

6.6 Développement durable

Lorsqu'une impression n'est pas nécessaire, autant éviter de gâcher du papier. Faire durer le matériel le plus longtemps possible est bon pour notre planète !