Chapitre 7 : Sécurisation des informations sensibles, Protection des données confidentielles et Préservation des nuisances.

I. Sauvegarde des données importantes :

I.1. Pourquoi faut-il sauvegarder :

Il existe quelques axiomes de base en informatique et notamment le fait que l'on doit toujours effectuer une copie de sauvegarde de ses informations importantes. Cette copie de sauvegarde doit bien évidemment s'effectuer sur un support physique indépendant de l'emplacement où le fichier original se situe ; en effet, il serait totalement inutile d'effectuer une copie de sauvegarde sur le même disque qui renferme le fichier original car, en cas de défaillance du disque, l'original et sa copie seraient perdus. Pratiquement, cela signifie que si l'on stocke ses fichiers sur son disque dur, ce qui est le cas le plus fréquent, il faut créer la copie de sauvegarde sur une disquette, un CD-R, une clé USB, un DVD-R, un disque amovible, un bureau virtuel, etc.

D'autres situations peuvent inciter l'utilisateur à faire une sauvegarde :

- Avant l'installation d'un nouveau logiciel afin de pouvoir revenir en arrière en cas de problème.
- Avant une intervention technique sur votre machine qui peut endommager le système.

I.2. Quelle fréquence de sauvegarde :

"L'utilisateur doit adopter un rythme de sauvegarde en fonction du caractère sensible de ses données et du rythme de modification.

S'il travaille très régulièrement sur les mêmes fichiers, il est nécessaire de faire une sauvegarde très régulièrement de ceux-ci afin d'éviter, en cas de perte, d'avoir à refaire un trop grand nombre de modifications. Si les données ont un caractère sensible (par exemple : les informations de tous les clients d'une entreprise, les commandes en cours, etc.), elles doivent être sauvegardées très souvent car une perte de celles-ci pourrait avoir des conséquences néfastes (par exemple : la faillite de l'entreprise).

I.3. Que doit-on sauvegarder :

Cela dépend de l'environnement (professionnel ou privé) et de l'importance que ces données présentent. Pour répondre à cette question, supposons que le disque dur de l'utilisateur tombe en panne et qu'il n'ait aucun moyen de récupérer les informations :

- Quelles données a-t-il définitivement perdues ? Ses photos de vacances, ses emails personnels, un rapport important, etc.
- Quelles sont celles qui lui sont utiles à court terme ? Ses favoris, ses adresses emails et numéros de téléphone de ses amis, collègues ou clients, etc.

I.4. Des méthodes de sauvegarde :

Dans ce paragraphe, nous allons voir différentes méthodes de sauvegarde.

I.4.1. Simple copie sur support amovible

La manière la plus courante de préserver des données est d'effectuer une sauvegarde sur un support amovible (CD-ROM, ZIP, JAZ, clé USB). Après avoir inséré le support celui-ci apparaît comme un nouveau disque amovible disponible sur votre machine, il suffit ensuite de faire, par exemple, une simple copie des répertoires à sauvegarder.

Cette façon de faire est très simple mais elle a trois défauts majeurs :

- L'utilisateur doit penser à renouveler cette action relativement souvent.
- Si ses données sont réparties dans un nombre de répertoires important, il peut arriver d'oublier de sauvegarder certains d'entre eux.
- Les données sont recopiées systématiquement même celles qui n'ont pas changées. Cela utilise de la place de manière excessive et augmente le temps passé à faire la sauvegarde.

I.4.2. Le mirroring :

Le mirroring (ou disque en miroir) a pour but de dupliquer l'information à stocker sur plusieurs disques simultanément. Ce procédé est basé sur la technologie RAID (acronyme de Redundant Array of Inexpensive Disks, traduire ensemble redondant de disques indépendants) qui permet de constituer une unité de stockage à partir de plusieurs disques durs.

L'unité ainsi créée (appelée grappe) a une grande tolérance aux pannes et possède une haute disponibilité. En effet, on obtient ainsi une plus grande sécurité des données, car si l'un des disques tombe en panne, les données sont sauvegardées sur l'autre. D'autre part, la lecture peut être beaucoup plus rapide lorsque les deux disques sont en fonctionnement. Enfin, étant donné que chaque disque possède son propre contrôleur, le serveur peut continuer à fonctionner même lorsque l'un des disques tombe en panne, au même titre qu'un camion pourra continuer à rouler si un de ses pneus crève, car il en a plusieurs sur chaque essieu.

En contrepartie ce procédé est très onéreux étant donné que seule la moitié de la capacité de stockage est utilisée de manière effective

I.4.3. Le backup :

Les logiciels de " backup " proposent de sauvegarder un ensemble de fichiers et de répertoires dans un fichier appelé archive. Ils offrent en général un grand nombre de fonctionnalités :

- Archivage et récupération des données.
- Compression des données.
- Planification des sauvegardes.
- Choix des différents répertoires et fichiers à sauvegarder.
- Choix de l'emplacement de l'archive : disque amovible, disque réseau, ...

II. Loi "Informatique et libertés" :

"La vie privée doit être murée, il n'est pas permis de chercher et de faire connaître ce qui se passe dans la maison d'un particulier." (Talleyrand)

Depuis son avènement, l'informatique a libéré l'être humain d'un nombre considérable de tâches pénibles et peu intéressantes. En devenant communicante, la micro-informatique a également permis d'autres libérations comme le télétravail. Mais cette mise en réseau des PC, qu'elle se fasse au sein de l'entreprise ou bien par l'intermédiaire d'Internet, a également des côtés négatifs que l'actualité vient nous rappeler régulièrement.

C'est une évidence de rappeler que chacun d'entre nous est fiché plusieurs centaines de fois et nous semblons avoir accepté cette situation avec la plus grande fatalité. Les belles âmes ont toujours d'excellentes justifications : il faut lutter contre la fraude fiscale, contre le piratage ou bien

encore le terrorisme. Si l'on peut être parfaitement d'accord avec le principe de la lutte contre le piratage ou bien l'échange illégal de fichiers musicaux, encore faut-il que ces combats soient menés de manière licite. Dans les faits que nous avons mentionnés, le plus répréhensible est bien évidemment le côté sournois et caché de ces procédures car si la loi Informatique et Libertés nous permet d'exercer un droit de regard sur les données nominatives qui ont été collectées, encore faut-il que nous soyons avertis que lesdites données ont été recueillies.

Comme nous allons le voir, il y a tout lieu de s'inquiéter du manque de respect de la vie privée sur Internet.

Notre propos n'est pas donc celui d'un moraliste, mais vise essentiellement à rappeler la et à faire réfléchir au pouvoir de l'informatique, ce qui implique la nécessaire élaboration d'un contre-pouvoir.

III. Dangers d'Internet :

III.1. Les virus informatiques :

Qu'est-ce qu'un virus informatique ?

Un virus informatique est un programme [des instructions écrites dans un langage de programmation] qui effectue certaines actions et, en général, cherche à se reproduire. Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté.

Les actions effectuées dépendent du virus et sont différentes d'un virus à l'autre : cela peut aller du simple affichage d'images ou de messages à l'écran à l'effacement complet du disque dur (dans ce cas, on parle de « bombe logique » ou de « charge utile »), en passant par la suppression de certains fichiers.

Les virus informatiques peuvent se répandre à travers tout moyen d'échange de données numériques comme l'Internet, mais aussi les disquettes, les cédéroms, ... 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.

IV. Le piratage informatique :

Les hackers :

Derrière le terme hacker, le grand public a souvent la vision d'adolescents en train de pirater les ordinateurs du FBI. La réalité est cependant un peu différente. Nous allons commencer par étudier l'origine de ce mot et voir qu'il existe différents types de hackers.

À l'origine, le mot hacker désigne celui qui se sert d'une hache, mais dans le contexte informatique, il semble que ce mot ait été employé pour la première fois au MIT, la célèbre université américaine. Un hacker est avant tout quelqu'un qui cherche à comprendre ce qui se passe sous le capot et qui étudie au plus près le fonctionnement interne d'un ordinateur, tant du point de vue matériel que logiciel.

En fait, un hacker désigne un passionné qui s'investit à fond dans son domaine de prédilection qui n'est pas forcément l'informatique.

Bien évidemment, à force de chercher dans les entrailles du système le hacker informaticien va découvrir des choses et fatalement quelques failles de sécurité. Mais ce n'est pas parce que le hacker met à jour une faille du système qu'il va l'exploiter ; pour désigner cette attitude, les hackers ont créé le terme cracker.

Un cracker est une personne qui cherche par tous les moyens à percer les systèmes de sécurité d'un logiciel ou d'un réseau.

V. Protection de la machine :

L'intrusion d'un autre utilisateur peut se faire soit par une prise en main directe de votre machine soit en passant par votre connexion réseau.

Ces deux points ont une réponse spécifique qui sont respectivement l'utilisation d'un mot de passe et d'un pare-feu.

V.1. Le mot de passe :

Actuellement tous les systèmes d'exploitation permettent à chaque utilisateur de protéger son espace de travail à l'aide d'un mot de passe de connexion associé à un nom de connexion (login). En plus de procurer une sécurité cela permet de créer un profil pour chaque utilisateur. Ce dernier peut ainsi personnaliser son espace de travail comme il le souhaite.

Si votre mot de passe est simple et court, il sera vite craqué !

➢ **Ce qu'il ne faut pas faire !**

- Il ne faut pas noter son mot de passe, choisissez donc un mot de passe facile à mémoriser.

- Il faut le garder secret. Si l'on désire travailler à plusieurs sur un même ordinateur, il faut créer autant de comptes que d'utilisateurs.

- Il ne faut pas choisir comme mot de passe une information personnelle (prénom, nom du projet...). Les mots présents dans un dictionnaire français ou étranger sont à éviter et à proscrire également toute variation de ce qui précède (ajout de chiffres, mots accolés, ...).

- Ne pas utiliser le même mot de passe pour tous ses besoins (accès machine, courrier, ftp, ...)

V.2. Comment choisir votre mot de passe :

- Utiliser un mot de passe suffisamment long : huit caractères est un minimum.

- Mélanger les différents types de caractères : lettres minuscules, majuscules, chiffres, ponctuation, caractères spéciaux.

- Etre imaginatif.

Il faut par ailleurs changer son mot de passe régulièrement, même s'il est très bon, tout simplement à cause du risque d'interception sur le réseau ou sur votre ordinateur. La fréquence de changement dépend de l'utilisation que vous faites de l'informatique et de votre environnement. Mieux vaut cependant changer son mot de passe moins souvent que de l'oublier.

VI. Protection contre les virus :

Pour les virus, nous pouvons comparer la relation qu'ils entretiennent avec les ordinateurs avec celle que les hommes entretiennent avec les virus biologiques. Nous savons en guérir mais si nous ne faisons pas attention nous en attrapons.

La solution la plus efficace pour ne pas attraper de virus ou pour s'en débarrasser est l'utilisation d'un anti-virus mais cela n'empêche pas l'utilisateur de rester vigilant.

Un antivirus est un logiciel qui possède une base de données recensant les morceaux de code des virus connus (*signatures*). Il comprend en général des composants suivants :

- *Un scanner* : programme qui permet de rechercher une éventuelle signature dans chaque fichier présent sur l'ordinateur.
- *Un gardien* : programme en mémoire qui analyse en temps réel tous les programmes manipulés par l'ordinateur. Ceux-ci peuvent être de simples applications lancées par l'utilisateur mais peuvent également se révéler être des virus tentant de se reproduire. Dans ce cas, si une signature est reconnue, le gardien alerte l'utilisateur en le prévenant qu'un virus est probablement actif sur l'ordinateur et empêche le virus de continuer son exécution.
- *Un module de mise à jour* automatique ou manuelle de la base de données de virus par connexion directe sur le site de l'éditeur du logiciel.

Le principe de fonctionnement d'un anti-virus est assez simple, il scanne ou surveille les fichiers de l'utilisateur et s'il détecte une signature de virus connu alors il peut en fonction de la stratégie adoptée par l'utilisateur :

- Désinfecter le fichier s'il le peut.
- Le mettre en quarantaine.
- Supprimer le fichier. *Attention* : cette action peut détruire des fichiers contenant des informations très importantes. Il faut donc l'utiliser avec prudence et parcimonie.

VII. Protection contre Les cybermenaces ou menaces en ligne :

VII.1. Les spywares :

Bien qu'à première vue anodin, le marché de la publicité sur Internet représente des sommes colossales qui expliquent cet acharnement à proposer aux annonceurs des services adaptés.

La fin justifiant les moyens, les sociétés éditrices de spywares n'hésitent pas à sacrifier la vie privée et la confidentialité des données des internautes sur l'autel du profit.

Les spywares ont pour but l'espionnage des habitudes de l'internaute dans le but de pouvoir cibler la publicité qui lui est proposée sur le web.

Le spyware a pour but de récolter un maximum d'informations sur l'utilisateur (les logiciels installés sur sa machine aussi bien que ses habitudes sur le web telles que les sites qu'il consulte, les publicités qui l'intéressent, etc.) et les envoyer vers un serveur où elles seront compilées et traitées.

Le spyware se charge en mémoire vive au démarrage de la machine et rapporte les moindres faits et gestes de l'internaute à son centre, de manière totalement invisible pour l'internaute.

VII.2. Les canulars (hoax)

Hoax Terme anglais qu'on peut traduire par canular, le hoax peut être défini comme une fausse information ou une rumeur. C'est une forme particulière de spam puisqu'il se base sur le courrier électronique. Il utilise la crédulité des utilisateurs pour se propager. En faisant circuler des informations qui apparaissent à l'utilisateur comme essentielles il compte sur celui-ci pour relayer (forwarder) l'information à tous ses contacts.

En général, le hoax n'est pas réellement dangereux puisqu'il ne met pas en défaut la sécurité des données de l'utilisateur et n'essaie pas de lui extorquer de l'argent. Cependant, le hoax possède quelques côtés pervers :

- Il sert la désinformation en faisant circuler de fausses informations ou des rumeurs non fondées et décrédibilise le moyen de diffusion que représente Internet.
- Il engorge les réseaux et les boîtes aux lettres en se servant des utilisateurs crédules pour être propagé.

Le site web www.hoaxbuster.com est une ressource en ligne recensant tous les hoax qui circulent sur Internet. Pour lutter contre la désinformation, pensez à toujours vérifier une information avant de l'envoyer à vos amis.

VII.3. Les chevaux de Troie

Le terme cheval de Troie (en anglais, trojan horse ou simplement trojan) tire bien entendu son origine d'un célèbre épisode de la mythologie grecque où un cheval en bois contenant des guerriers avait été introduit, grâce à une ruse, dans la ville de Troie assiégée.

Un cheval de Troie est donc un programme qui effectue une tâche spécifique à l'insu de l'utilisateur. À la différence d'un virus, un cheval de Troie ne se reproduit pas, mais de nombreux virus diffusent également un cheval de Troie sur l'ordinateur qu'ils infectent.

Un cheval de Troie peut être exécuté de manière furtive à chaque démarrage de l'ordinateur si un virus a programmé son exécution automatique en ajoutant des clés dans le registre.

Un cheval de Troie peut aussi se cacher dans un logiciel qui lui servira d'hôte.

VIII. Prévenir la perte de données :

Pour prévenir la perte de données vous devez paramétrer correctement votre corbeille, assurer le bon état de votre machine et assurer des sauvegardes régulières.

VIII.1. Paramétrer correctement sa corbeille :

Dans la partie précédente nous avons vu comment se protéger des virus. Mais l'utilisateur peut de lui-même provoquer la perte de données par un effacement accidentel. Pour éviter cela, ne jamais désactiver la corbeille. En effet, cette dernière stocke tous les fichiers effacés par l'utilisateur. Ainsi, un fichier effacé accidentellement peut être facilement récupéré. Les fichiers contenus dans la corbeille seront définitivement perdus lorsque l'utilisateur videra la corbeille.

VIII.2. Surveiller le bon état de votre machine :

Tous les accidents ne sont pas prévisibles mais l'utilisateur peut agir de manière à éviter certains désagréments. L'installation d'un onduleur évitera lors d'une coupure de courant la perte des données en cours d'utilisation. Il n'est pas uniquement destiné à pallier les coupures de courant, son rôle est également de stabiliser la tension électrique et d'éliminer les parasites qui sont des causes éventuelles de pannes matérielles. L'arrêt de la machine ou la mise en veille lorsque l'on ne l'utilise pas, évitera une fatigue prématurée des disques durs et abaissera le risque de panne surtout lors des fortes chaleurs.

VIII.3. Assurer une sauvegarde :

La meilleure façon de prévenir la perte de données est d'assurer une sauvegarde régulière de vos données personnelles.

IX. La cryptologie :

Parler de cryptologie est un exercice très délicat.

Dans l'esprit du grand public, la cryptographie évoque souvent l'image des casseurs de code mythiques comme Alan Turing qui réussit à déchiffrer le code de l'Enigma, ce qui permit aux alliés de débarquer un an plus tôt en Normandie pendant la Deuxième Guerre mondiale.

Pour les spécialistes, la cryptologie n'est qu'une affaire de factorisation et de nombres premiers ; ne dit-on pas d'ailleurs que le premier employeur de mathématiciens au monde est la NSA (National Security Agency), le service de renseignements américain qui pilote le programme d'écoute Echelon ?

L'usage de la cryptographie a longtemps été réservé en France aux gens qui sont chargés de préparer la guerre, à savoir les militaires. Les politiques ayant finalement compris que ces restrictions législatives étaient un frein énorme au développement du commerce électronique, la loi a été modifiée et les moyens cryptographiques ne sont plus désormais considérés comme des armes de guerre.

Quand on conseille à un utilisateur d'employer un outil de cryptographie, son premier réflexe est de prétendre qu'il n'a rien à cacher. Quand bien même cela serait vrai (ce qui reste encore à prouver...), nous allons voir que les enjeux de la cryptographie sont tout autres et que *la cryptologie est aujourd'hui au centre de toute démarche sécuritaire en informatique*.

X. La signature électronique :

Il y a encore peu de temps, la signature électronique n'était qu'un concept que la plupart des gens appréhendaient mal ; or, aujourd'hui, il s'agit d'une réalité qui va révolutionner la vie quotidienne des particuliers et des entreprises.

La signature électronique est un dispositif cryptographique qui permet de s'assurer de l'identité de la personne qui signe le courrier. En fait, signer un courrier électroniquement, c'est fournir un

code secret qui authentifie l'auteur du message, de la même manière que le code secret de votre carte bancaire permet au distributeur de billets de savoir que c'est bien vous qui retirez de l'argent.

Ce nouveau concept est rendu possible grâce à l'évolution des moyens cryptographiques, ainsi qu'à l'adaptation de la législation. L'application la plus immédiate de la signature électronique est que l'on peut signer un document numériquement et l'envoyer par courrier électronique, là où il fallait auparavant prendre un stylo, signer au bas de la feuille et envoyer le document papier par la Poste.

Juridiquement, la signature électronique a la même valeur que la signature manuscrite, dès lors qu'elle permet de garantir :

- *L'identité du signataire* : la signature d'une personne exprimant son consentement, il est essentiel de pouvoir affirmer avec certitude que la signature électronique a bien été apposée par cette personne (et non par une autre) ;
- *L'intégrité du document sur lequel a été apposé la signature* : une personne ne signe un document que parce qu'elle est d'accord avec ce qu'il contient. Il est donc impératif de garantir que le contenu ne pourra pas être modifié après signature ;
- *L'indissociabilité de la signature et du document signé* : il ne doit pas être possible d'extraire la signature électronique apposée par une personne sur un document pour l'intégrer à un autre document.