La sécurité des postes clients

DA2I

Poste client

- Poste client
  - Système informatique mis à la disposition des utilisateurs
    - Poste fixe
    - Poste nomade (ordinateur portable), avec des **risques** supplémentaires
  - Système d'exploitation utilisé majoritairement : Windows
- Caractéristiques communes entre le poste client de l'entreprise et l'ordinateur personnel: Le poste de travail professionnel peut parfois être utilisé à des fins personnelles

  Ex: consulter sa banque en ligne depuis son lieu de travail

Vulnérabilités

- Vulnérabilités système
  - Exploitées de façon automatique via l'Internet, lorsqu'il s'agit de vulnérabilités exploitables à distance et de façon anonyme
  - Par la suite, exploitées par les vers
- Vulnérabilités du poste client
  - Tirer parti des vulnérabilités des applications installées communément : Applications intégrées, fonctions cœur du système …
- Vulnérabilités de l'infrastructure
  - Utilisateur à privilèges → Systèmes de protection moins efficaces
  - Contournement des mesures de filtrage

Menaces

- Logiciel malveillant (Malwares)
  - Modification de données : perte d'intégrité
  - Vol d'informations : perte de confidentialité
  - Déni de service : perte de disponibilité
- Attaques ciblées pour le profit :
  - Pénétrer dans un Système d'information pour voler, modifier, entraver …
- Vol :
  - Oubli d'un ordinateur portable dans un taxi
  - Machine laissée sans surveillance dans une salle

    → Perte de **disponibilité**

    → Potentielle perte de **confidentialité**

Logiciel malveillant (malware)

Un logiciel malveillant est un logiciel développé dans le but de nuire à un système informatique.

- le **virus** : programme se dupliquant automatiquement sur le même ordinateur. Il peut être transmis à un autre ordinateur par l'intermédiaire du courrier électronique ou par l'échange de données ;
- le **ver** (*worm*) : exploite les communications réseaux d'un ordinateur afin d'assurer sa reproduction sur d'autres ordinateurs ;
- le **cheval de Troie** (*trojan*) : programme à apparence légitime (voulue) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur ;
- la **porte dérobée** (*backdoor*) : permet d'ouvrir un accès réseau frauduleux sur un système informatique. Il est ainsi possible d'exploiter à distance la machine ;
- le **logiciel espion** (*spyware*) : fait de la collecte d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation. Ces informations sont ensuite transmises à un ordinateur tiers ;
- **l'enregistreur de frappe** (*keylogger*) : programme généralement invisible installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier ; pour intercepter des mots de passe par exemple.

Les modes de contamination

Pour pouvoir se propager, les parasites informatiques ont besoin d'utiliser des supports physiques.

A - Les supports amovibles: Tout support qui a besoin d'être connecté ou introduit dans un ordinateur est un danger potentiel.

- **La disquette** : support le plus ancien, la disquette permet de sauvegarder les fichiers d'un ordinateur puis de les restaurer sur un second. Si les fichiers de la première machine sont infectés par un virus, la copie sur la disquette copiera le virus qui se retrouvera ensuite sur le second poste.
- **Le CD-ROM** : support de plus grande capacité, on y trouvait au début des programmes vendus par les éditeurs de logiciels. Certains programmes comportaient des virus. Aujourd'hui les CD-ROM et DVD-ROM sont devenus inscriptibles ou réinscriptibles et deviennent un facteur de propagation identique aux disquettes.
- **La clef USB**: Il s'agit d'une mémoire réinscriptible de capacité plus élevée. Elle remplace la disquette et peut aussi contaminer un ordinateur.

B - Le réseau informatique: La plus grande partie des infections est réalisée aujourd'hui par les réseaux.

- **Réseau local**: une seule machine infectée transmet par le réseau le parasite à l'ensemble des ordinateurs.
- **Réseau Internet** : la messagerie électronique, que ce soit par un message au format HTML ou une pièce jointe va permettre de diffuser le parasite en utilisant des adresses de destinataires contenues dans le carnet d'adresses de l'ordinateur.

Les dommages

Si certains parasites sont inoffensifs, d'autres ont un comportement beaucoup plus nuisible et préjudiciable pour les données et parfois pour la machine elle-même.

- **Destruction de fichiers** : elle peut être partielle en s'attaquant à un type de fichiers (programme, document, image, son) ou totale lors d'un formatage du support.
- **Corruption de fichiers** : l'objectif est de modifier la structure du fichier pour le rendre inutilisable: caractères parasites dans un document, son inaudible, images dégradées, programme inutilisable. Lorsqu'il s'agit de données de gestion, le coût pour une organisation peut être très élevé.
- **Destruction matérielle** : certains virus vont exécuter des instructions à répétition pour provoquer un échauffement qui détruira un composant ou bien détruire le programme qui gère les entrées-sorties d'information (BIOS) de la carte mère d'un ordinateur. L'appareil est détruit sans savoir s'il s'agit d'une panne matérielle ou d'un acte volontaire de destruction.
- **Instabilité du système** : d'autres virus rendent le système instable par un blocage aléatoire qui oblige à redémarrer l'ordinateur.
- **Dégradation des ressources du système** : le virus utilise les ressources de l'ordinateur (mémoire, disque dur) pour se répliquer, il ralentit le système jusqu'au blocage complet par saturation des disques ou de la mémoire.
- **Compromission des paramètres de sécurité** : il s'agit d'une action courante des chevaux de Troie qui installe des modules pour intercepter les frappes au clavier (KeyLogger) notamment les mots de passe et les envoyer vers une machine à l'extérieur du réseau.
- **Blocage de la sécurité :** le virus s'attaque aux programmes anti-virus ou pare-feu en les désactivant pour les empêcher de fonctionner.

Virus

- **Définition:** *Un **virus** est un programme informatique, situé dans le corps d'un autre programme qui modifie le fonctionnement de l'ordinateur à l'insu de l'utilisateur.*

- Il se propage par **duplication**. Pour cela, il va infecter d'autres programmes d'ordinateur en les modifiant de façon à ce qu'ils puissent à leur tour se dupliquer.

- Il agit lorsqu'il est chargé en mémoire au moment de l'exécution du logiciel infecté.

- La plupart des virus **visent à déclencher une action**. Certaines actions sont sans danger : affichage d'un message, exécution d'une musique, dessin sur l'écran, etc. D'autres ont une action beaucoup plus nuisible.

Virus : Quelques éléments

- **Méthodes d'infection :**
  - Messagerie électronique, …
  - Disquettes, CD, …
  - Partage réseau
  - Vulnérabilité des systèmes
  - …
- **Plates-formes vulnérables :**
  - Actuellement Windows
  - Mais les autres systèmes n'en seront peut-être pas exempt éternellement (Unix, Macintosh, …)

Les différentes familles de virus

- On distingue plusieurs catégories de virus, en fonction de la cible visée dans l'ordinateur:
  - Les virus d'applications
  - Les virus système
  - Les virus macro
  - Les virus de mail (vers)
  - Virus de script

Virus d'application

- Le virus programme (ou virus d'application) infecte les programmes exécutables. Il se glisse dans une partie du code et sera exécuté en même temps que l'application.
- Le virus remplace l'amorce du fichier, de manière à ce qu'il soit exécuté avant le programme infecté, puis il lui rend la main, camouflant ainsi son exécution aux yeux de l'utilisateur.
- Il en profitera pour se reproduire, contaminer d'autres exécutables et déclencher l'action prédéterminée par son auteur.

Virus système

- Le **virus système** (ou **virus de secteur d'amorce)** infecte la zone du disque durs qui est lue en premier au démarrage (secteur d'amorçage);
- remplace le secteur d'amorçage du disque infecté, puis déplacent le secteur original vers une autre portion du disque;
- Le virus est ainsi chargé en mémoire bien avant que l'utilisateur ou un logiciel ne prenne le contrôle de l'ordinateur;
- Exemple de ces virus: Form, jack the ripper, french boot, parity boot…

Virus macro

- Le **virus macro** est un virus qui infecte les documents (Word, Excel, etc…).
- Il est possible d'insérer dans un document des actions programmées pour automatiser certaines tâches : création de formulaires, mises en forme automatisées, etc..
- Ces tâches sont réalisées à l'aide d'un langage de programmation (Visual Basic pour les applications de la suite Office de Microsoft). Le virus se sert de ce langage pour se reproduire et déclencher une action destructrice.

Les virus de mail (vers)

- Ces virus se servent des programmes de messagerie pour se répandre à grande vitesse, en s'envoyant automatiquement à tout ou partie des personnes présentes dans le carnet d'adresses.
- Leur premier effet est de saturer les serveurs de messagerie;
- Ils peuvent également avoir des actions destructrices pour les ordinateurs contaminés;
- Ils sont particulièrement redoutables, car le fait de recevoir un mail d'une personne connue diminue la méfiance du destinataire, qui ouvre alors plus facilement le fichier joint contaminé.
- Le ver est une variante de virus qui a la particularité de ne pas avoir besoin de support pour se reproduire, il se suffit à lui-même.

Virus de script

- Le **virus de script** infecte les pages HTML chargées par un internaute.
- Une page HTML est composée de balises interprétées par le navigateur. Il est possible d'ajouter dans une page HTML des programmes écrits dans un autre langage pour enrichir les pages et les rendre dynamiques.
- Les plus utilisés sont VB-Script et JavaScript. VB-Script est à l'origine de nombreux virus.

Virus : Conséquences

- Envoi de messages « publicitaires » (SPAM)
- Envoi de fichiers personnels
- Ajout, destruction ou modification de fichiers
- Désactivation de logiciel de sécurité tels que Antivirus, garde-barrière…
- Installation de porte dérobée
- Écoute du trafic
  - Vol de mot de passe

Comment savoir si mon ordinateur est contaminé ?

- **Les virus sont le plus souvent repérés trop tard, par les conséquences potentiellement désastreuses de leur activité.**

- **Il existe toute une série d'indices qui peuvent indiquer l'infection de l'ordinateur par exemple:**
  - **mémoire système disponible inférieure à ce qu'elle devrait être,**
  - **changement du nom de volume d'un disque,**
  - **programmes ou fichiers subitement absents,**
  - **L'affichage à l'écran de messages ou de dessins inhabituels ou l'émission de sons étranges ;**
  - **Le lancement aléatoire d'une application quelconque sans l'intervention de l'utilisateur ;**
  - **Vos amis ou vos connaissances parlent de vos messages alors que vous ne leur avez rien envoyé ;**
  - **ou encore comportement anormal de certains programmes ou fichiers.**

Règles générales de protection des virus

Quelques règles simples peuvent être appliquées :

- **ne téléchargez pas des programmes d'origine douteuse, qui peuvent vous être proposés sur des sites « perso » ou origines douteuses;**
- **méfiez-vous des fichiers joints aux messages que vous recevez:**
  - **analysez avec un antivirus à jour tout fichier avant de l'ouvrir,**
  - **préférez détruire un mail douteux plutôt que d'infecter votre machine, même si l'expéditeur est connu;**
- **analyser les disquettes ou flash d'origine douteuse (ou ayant transité dans des lieux publics vulnérables des écoles ou universités), et protégez les vôtres en écriture;**
- **procédez régulièrement à des sauvegardes du contenu important de votre disque dur après avoir vérifié l'absence de virus;**
- **tenez-vous au courant des apparitions de nouveaux virus. Secuser.com vous offre ce service en émettant des alertes lorsqu'un virus connaît une diffusion importante.**

Que faire en cas de contamination ?

- La solution la plus simple reste de vous procurer un logiciel antivirus pour procéder immédiatement à l'analyse et l'éradication de virus présents sur vos disques.

- En cas de contamination par un virus de boot ou un virus de fichier :

    1. Si votre machine n'est pas configurée en multi-boot, utiliser un outil (fdisk/mbr) pour supprimer le Master Boot Record (secteur d'amorce du PC, automatiquement régénéré au prochain démarrage);

    2. Eteignez l'ordinateur (pas reset, ni redémarrage);

    3. Démarrez à partir d'un disque de boot sain (cd-rom ou flash disque par exemple), protégée en écriture, et contenant un antivirus;

    4. Lancez l'antivirus (le reste dépend de l'antivirus).

Que faire en cas de contamination? (2)

Pour les virus macro**:**

- il est conseillé de rechercher le fichier normal.dot et de le supprimer, puis ensuite de détruire tous vos documents.
- Cette méthode supprime les virus macro définitivement, mais aussi malheureusement votre travail.
- Une solution consiste à utiliser un "bloqueur" lorsque vous chargez un document inconnu:
  - ce type de programme empêche le transfert de nouveaux virus dans vos autres documents.

Le cheval de Troie

- **Définition :** *Le cheval de Troie, aussi connu sous le nom anglais de Trojan Horse ou simplement trojan, est une des méthodes les plus courantes d'intrusion dans un système. Un cheval de Troie est un programme d'apparence bénigne ouvrant une brèche de sécurité à des fins malicieuses.*

- Un cheval de Troie est un programme qui se présente sous une forme anodine (mail, bandeau publicitaire, jeu en téléchargement) mais qui contient en réalité des instructions cachées, dans le but de pénétrer par effraction dans des fichiers pour les consulter, les transférer, les modifier ou les détruire .

- Il permet à un pirate de s'introduire dans une machine sans le consentement de l'utilisateur. Dans ce cas, il insère un logiciel "serveur" qui offrira au pirate toutes les informations dont il a besoin.

- Le pirate pourra prendre le contrôle à distance de l'ordinateur infecté. À la différence d'un virus, il ne cherche pas à se reproduire. L'objectif est de récupérer des informations confidentielles : codes de carte bancaire, identifiant et mots de passe, documents personnels.

- **Le cheval de Troie est** avant tout **un moyen de transport d'un parasite** plus ou moins dangereux. Il utilise souvent une faille de sécurité pour s'introduire dans un ordinateur.

Le cheval de Troie: Conséquences

Le cheval de Troie est potentiel nuisible :

- Les dommages causés par un cheval de Troie peuvent avoir des conséquences très sérieuses. Il peut donner l'entier contrôle de votre système à de parfaits inconnus agissant sous le couvert de l'anonymat. Par exemple, le contenu de votre système pourrait être totalement supprimé.
- De façon plus insidieuse, vos données personnelles ou d'affaires sur votre ordinateur pourraient être découverts et dans certains cas modifiés.
- Sans que vous ne vous doutiez de rien, un cheval de Troie peut permettre à un pirate informatique d'utiliser votre identité pour commettre des délits criminels dont l'enquête remontera jusqu'à vous.

Le cheval de Troie: Conséquences

Le cheval de Troie est potentiel nuisible :

- Les dommages causés par un cheval de Troie peuvent avoir des conséquences très sérieuses. Il peut donner l'entier contrôle de votre système à de parfaits inconnus agissant sous le couvert de l'anonymat. Par exemple, le contenu de votre système pourrait être totalement supprimé.

- De façon plus insidieuse, vos données personnelles ou d'affaires sur votre ordinateur pourraient être découverts et dans certains cas modifiés. Ainsi le vol de renseignements personnels : informations bancaires, mots de passe, codes de sécurité…

- Sans que vous ne vous doutiez de rien, un cheval de Troie peut permettre à un pirate informatique d'utiliser votre identité pour commettre des délits criminels dont l'enquête remontera jusqu'à vous.

- Suppression, modification ou transfert de fichiers (téléchargement ou upload).

Le cheval de Troie: Symptômes possibles d'une infection

- Un comportement inhabituel dans le fonctionnement de l'ordinateur, tels que:
- Activité anormale de la carte réseau ou du disque dur (des données sont chargées en l'absence d'activité de la part de l'utilisateur)
- Plantages répétés
- Redémarrage répété du système
- Réactions curieuses de la souris
- Ouvertures impromptues de programmes, du lecteur CD/DVD
- Écran ou fenêtres avec des messages inhabituels.
- Ouverture/Fermeture intempestive de fenêtres.
- Le navigateur accède tout seul à certains sites Internet.
- Présence d'autres programmes qui n'ont pas été volontairement installés (y compris des logiciels malveillants).
- …

Le cheval de Troie: quelques exemples

- **Back Orifice:** s'installe sur le systèmes Windows comme une application client/serveur pour l'administration à distance par un groupe se donnant le nom de Cult of the Dead Cow, il s'agit en fait d'un programme très dangereux. Il permet aux pirates qui l'exploitent de faire à distance, et dans l'anonymat, tout ce que vous pouvez faire vous-même au clavier de votre ordinateur

- **B**ack Orifice ouvre des ports de communication qui peuvent être connus de la plupart des pirates, permettant ainsi à quiconque sachant comment s'y prendre d'entrer dans votre système. Il est également possible de spécifier les ports de communication et d'en protéger l'accès par un nom d'utilisateur et un mot de passe. Le pirate se réserve ainsi l'exploitation illicite de votre système sans que vous ne soyez même conscient de sa présenc.

- **NetBus et autres :** NetBus est un autre cheval de Troie très répandu. Tout comme Back Orifice, il s'installe insidieusement sur votre ordinateur pour ouvrir des portes d'entrées à qui veut bien les exploiter. Selon les versions, NetBus crée une des entrées suivantes dans la base de registre de Windows : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ou HKEY_CURRENT_USER\NetBus Server. Une des caractéristiques de NetBus est de permettre à un pirate d'ouvrir et fermer la porte de votre lecteur de cédérom à distance. Si vous constatez un tel comportement erratique sans raison apparente, il vaudrait mieux faire une **vérification** de votre système :

Le cheval de Troie: comment se protéger

- Les erreurs à éviter pour se protéger contre les chevaux de Troie et les **virus** sont les mêmes.

- Bien qu'ils diffèrent des **virus** par leur mode de propagation, les chevaux de Troie sont maintenant détectés par bon nombre de **logiciels anti-virus**. Certains logiciels sont toutefois spécialisés uniquement dans la protection contre les chevaux de Troie.

- En premier lieu, n'acceptez **jamais** d'exécuter des programmes qui ne viennent pas d'une source entièrement sûre.

Les espiogiciels (spyware)

- **Définition:** *Logiciel introduit dans un ordinateur sans l'autorisation explicite de son utilisateur pour collecter des informations et les transmettre à un tiers.*
- **Des buts différents :**
  - Constitution de profil d'internautes pour des régies publicitaires
  - Espionnage industriel
  - Introduction de chevaux de Troie par des pirates
- Ces logiciels sont parfois présentés par des sociétés commerciales comme des outils de suivi des habitudes d'un utilisateur dans le but d'améliorer les produits de la société, mais cette collecte effectuée sans le consentement de l'utilisateur est une intrusion dans la vie privée.
- On les trouve notamment dans les bandeaux publicitaires de page HTML, dans les logiciels de téléchargement et d'échange de morceaux de musique.

Les espiogiciels: Diffusion

- Les logiciels espions sont souvent inclus dans des logiciels gratuits et s'installent généralement à l'insu de l'utilisateur.
- L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.
- Certains sont cachés et ne se retrouvent donc pas dans la table des processus (accès : {Ctrl+alt+suppr} pour Windows, {ps} pour Unix).
- Un logiciel anti-espion performant peut toutefois les détecter et envoie une alerte avant leur installation.

Les espiogiciels: Fonctionnement

Un logiciel espion est composé de trois mécanismes distincts :

- Le mécanisme d'infection, qui installe le logiciel:
  - Ce mécanisme est identique à celui utilisé par les virus, les vers.
  - Par exemple, l'espiogiciel Cydoor utilise le logiciel grand public Kazaa comme vecteur d'infection ;
- Le mécanisme assurant la collecte d'information:
  - Pare exemple l'espiogiciel Cydoor, la collecte consiste à enregistrer tout ce que l'utilisateur recherche et télécharge via le logiciel Kazaa.
- Le mécanisme assurant la transmission à un tiers:
  - Ce mécanisme est généralement assuré via le réseau Internet.
  - Le tiers peut être le concepteur du programme ou une entreprise.

Les espiogiciels: *Risques*

- Moyen de collecter des adresses électroniques / SPAM
- Le logiciel espion peut:
  - afficher des offres publicitaires, télécharger un virus, …
  - capturer des mots de passe en enregistrant les touches pressées au clavier (*keyloggers*),
  - espionner les programmes exécutés à telle ou telle heure, ou encore espionner les sites Internet visités,
  - Récupération de données sensibles, personnelles, …
  - …

Le Spam

- **Définition:** *Le spam (ou pourriel) est un courrier électronique abusif et indésirable.*

- Le spam se réfère aux courriers électroniques publicitaires envoyés en masse à des milliers d'internautes qui n'ont pas donné leur accord pour les recevoir. On surnomme les émetteurs de ces messages «**spammeurs**».

- Intérêt de cette pratique pour les expéditeurs:
  - Il s'agit d'un procédé très peu coûteux pour expédier des offres commerciales à des millions d'adresses.
  - Des logiciels spécialisés appelés « robots » parcourent le Web pour y récupérer les adresses. L'envoi des courriels est quasiment gratuit.

Le Spam

- Le spam présente deux inconvénients majeurs:
  - Il parasite Internet, en monopolisant une grande partie du trafic du courrier électronique
  - dévalorise les démarches commerciales responsables sur Internet.

- Les acteurs de l'Internet s'efforcent donc de limiter le phénomène par des moyens techniques, et les états tentent d'y mettre fin par des dispositions législatives. Mais l'aspect international du phénomène et l'inventivité des spammeurs rendent l'éradication du fléau très difficile.

Les canulars

Définition: *Un canular (en anglais hoax) est une annonce reçue par mail qui incite à transférer ce message à tous les contacts contenus dans le carnet d'adresses.*

Variété des canulars:

- **Arrivée d'un danger :** le message prévient d'un danger, l'arrivée d'un nouveau virus (faux virus), il se sert de la caution de sociétés renommées pour appuyer ces affirmations.
- **Les chaînes de solidarité** : il encourage à sauver une ou plusieurs personnes atteintes d'une maladie rare, il fait appel à la générosité des internautes.
- **Un gain potentiel** : le message promet de gagner beaucoup d'argent en très peu de temps. Le message est parfois étayé d'un exemple extravagant (gagner plusieurs milliers de dollars).
- **Bonne ou Mauvaise fortune** : Le message vous prévient de la bonne fortune ou du malheur le plus terrible si vous ne le faites pas suivre. On cite l'exemple d'une personne qui n'a pas renvoyé le message et qui a eu tous les malheurs du monde jusqu'à ce qu'elle se décide, ses problèmes se sont alors tous immédiatement résolus.
- **Désinformation:** Le message "prévient" d'un fait généralement scandaleux et vise à faire réagir le destinataire et réclame la diffusion la plus large possible.

Les mécanismes de protection

- Pour protéger son poste, il importe de disposer de logiciels qui vont empêcher toute action nuisible et éventuellement neutraliser un programme dangereux.

- Les principaux mécanismes utilisés sont :
  1. La mise à jour des programmes
  2. Sauvegarder ses données
  3. L'anti-virus
  4. Pare-feu

La mise à jour des programmes

Beaucoup de programmes comportent des bogues ou des failles de sécurité dont se servent les parasites pour se propager et infecter les ordinateurs. Les mises à jour concernent aussi bien le système d'exploitation que les programmes applicatifs.

1. Le système d'exploitation

- La course à des produits toujours plus performants conduit les éditeurs à mettre sur le marché de nouveaux systèmes d'exploitation ou de nouvelles versions insuffisamment testés. Très rapidement des failles de sécurité sont découvertes qui entraînent la publication de correctifs.
- Lorsqu'une machine n'est pas à jour de ces correctifs elle devient une cible potentielle pour tout type d'attaque.
- Il est donc impératif de mettre à jour le système d'exploitation. Cette mise à jour peut être manuelle ou automatisées.

2. Les logiciels applicatifs

- Les navigateurs Internet, les clients de messagerie et les logiciels métiers comportent eux aussi des failles de sécurité. Leur correction obéit aux mêmes principes que le système d'exploitation.
- Les mises à jour peuvent être couplées avec le système d'exploitation lorsqu'il s'agit du même éditeur ou bien réalisées séparément sur le site Internet de l'auteur du logiciel.

Sauvegarder ses données

- La sauvegarde est une protection contre les parasites et les autres risques: pannes matérielles, vol, malveillance interne, accident, etc …
- Pour être efficace les sauvegardes doivent remplir plusieurs conditions:
  - être régulières, le rythme est fonction de l'importance des données et de leurs modifications.
  - être réalisées sur un support fiable : bande magnétique, disque dur externe, CD non réinscriptible. Les disquettes et clefs USB sont considérées plus comme un moyen de transport que comme un outils d'archivage. Les CD réinscriptibles offrent moins de fiabilité que les gravures définitives.
  - être stockées dans un endroit différent de celui où est situé le poste de travail.

Les anti-virus

- **L'anti-virus :** *Programme qui empêche les virus de contaminer un ordinateur.* Il peut parfois neutraliser un virus déjà présent. Le rôle essentiel d'un anti-virus est d'interdire l'arrivée d'un virus dans la machine. Si le virus a réussi à pénétrer à l'intérieur du système, l'action de l'anti-virus sera beaucoup moins efficace.

- **Pour être efficace un anti-virus doit**
  - **être présent sur la machine** avant toute source de contamination ;
  - **être à jour** : base anti-virale et moteur de détection ;
  - **être actif en permanence**.

Les anti-virus : Fonctionnement

- Dés qu'un virus tente de pénétrer dans l'ordinateur, l'anti-virus va, en fonction du type de danger :
  - **supprimer** (nettoyer) la partie du code correspondant au virus dans le fichier infecté, le fichier pourra alors être normalement utilisé.
  - **supprimer le fichier infecté** si celui-ci ne peut pas être nettoyé ou si l'intégralité du code est néfaste;
  - **mettre en quarantaine le fichier infecté**, c'est-à-dire déplacer le fichier dans un emplacement contrôlé par l'anti-virus pour l'empêcher de se déclencher.

- Ces actions peuvent être automatisées en fonction des réglages du logiciel. Il est donc préférable de vérifier dés l'installation les paramètres par défaut et d'adapter les actions du logiciel en fonction de la politique de sécurité que l'on souhaite implanter sur l'ordinateur. Les logiciels sont très souvent prudents dans leurs actions

Les anti-virus: Technologie

- Les anti-virus utilisent différentes technologies pour rechercher les virus :
  - **La recherche de signatures:**
    - Le logiciel analyse les fichiers pour détecter la présence d'un virus. Pour que cette méthode soit efficace il faut que la base des signatures soit régulièrement mise à jour.
    - Cette méthode ne permet pas de détecter les virus qui utilisent une nouvelle signature, mais la rapidité de réaction entre la découverte d'un nouveau virus et la mise à jour de la base permet d'arrêter la plupart des virus.
  - **La méthode heuristique** :
    - elle consiste à chercher des instructions suspectes à l'intérieur des fichiers en se basant sur des règles générales de reconnaissance des virus.
    - Cela permet de détecter aussi bien des virus connus qu'inconnus, sans effectuer de fréquentes mises à jour.
    - Toutefois, cette méthode génère parfois de fausses alertes. L'utilisateur doit être capable de faire la différence entre les vraies et les fausses alertes.
  - **Le contrôle d'intégrité** :
    - lors de son installation, l'antivirus crée une base de données de tous les fichiers présents sur la machine basée sur la longueur des fichiers et d'autres paramètres.
    - Toute modification d'un fichier fera l'objet d'une alerte.
- Les logiciels antivirus combinent ces méthodes pour proposer des produits aussi performants que possible.

3. Le pare-feu

- **Définition:** *Un pare-feu (firewall en anglais), est un logiciel permettant de protéger un ordinateur des intrusions provenant d'un réseau.*

- Il doit protéger aussi bien le poste des attaques provenant d'Internet que celles provenant d'un réseau interne..

Précautions (1)

- Il n'existe pas de système informatique complètement sécurisé mais quelques mesures simples permettent d'éloigner le risque de perdre tout ou partie des données dont on a la responsabilité.
- **Adopter un comportement sans risque:** Quelques mesures simples permettent à un utilisateur d'éviter d'être une cible potentielle.

Au niveau du service informatique

- **Mettre en place une architecture sécurisée**
- **Mettre un antivirus sur les postes et sur le flux SMTP (au minimum)**
- **Mettre à la disposition des utilisateurs**
  - **Logiciels anti-virus, anti-spyware, …**
- **Informer et sensibiliser les utilisateurs**
  - **Avis de sécurité, virus, …**
  - **Vulnérabilités, …**

Précautions (2)

Au niveau de chaque poste de travail

- **Mettre à jour régulièrement :**
  - **Système d'exploitation**
  - **Logiciel**
- **Choisir de bons mots de passe**
- **Désactiver au maximum :**
  - **Tout ce qui est réputé dangereux (compte invité,…)**
  - **Tout ce qui est inutile sur un poste client**
- **Installer un anti-virus et éventuellement un par-feu.**

Précautions (3)

Sauvegarder les données

- **Fournir des moyens de sauvegarde aux postes clients :**
  - **Disque partagé sur le serveur**
  - **Disque externe, graveur de CD, etc.**
- **Mettre les sauvegardes dans un lieu sûr !**
- **Sensibiliser et former les utilisateurs :**
  - **Informations à sauvegarder**
  - **Fréquence de sauvegarde**
  - **Restauration**

Précautions (4)

- **Quelques idées :**
  - **Choisir un bon mot de passe**
  - **Ne pas coller son mot de passe sous le clavier**
  - **Ne pas installer de logiciels piratés**
  - **Ne pas modifier les configurations définies**
- **Au niveau du système**
  - **Activer le verrouillage automatique de l'écran**
  - **Manipuler avec précaution les partages de fichier**
  - **…**

Précautions (5)

- **Ne pas diffuser inutilement son adresse sur Internet.**
- Lorsqu'on reçoit du spam, c'est que l'adresse que l'on possède circule sur le réseau Internet.
- Des programmes malveillants parcourent en permanence pages visibles sur le Web à la recherche d'adresses de messagerie. Or une adresse peut apparaître sur une page Web à différentes occasions : la signature d'un article, une contribution dans un forum, la saisie dans un formulaire, un annuaire public,….
- Pour toutes ces raisons, il est préférable d'utiliser un compte de messagerie dédié aux activités exposées et conserver une autre adresse pour les échanges professionnels ou personnels.

Précautions (6)

- **Ne pas répondre à un expéditeur inconnu.**
  - Une bonne part des messages non désirés sont en réalité des adresses usurpées dont le véritable expéditeur cherche à contaminer une machine. Parfois il arrive que l'expéditeur soit une personne connue dont l'adresse est falsifiée, le nom de l'expéditeur est connu mais l'email n'est pas le bon.
  - Il faut s'intéresser au contenu du message qui est très souvent en complet décalage avec la personne sensée avoir expédié le message.
  - Lorsqu'une pièce jointe accompagne le message, il faut s'assurer qu'elle est explicitement déclarée dans le message et en rapport avec l'activité de l'expéditeur.
- **Ne jamais transférer un message à tout son carnet d'adresses**
  - Cette pratique encouragée par le spam est à éviter absolument. Elle encombre la messagerie, elle divulgue à chacun l'intégralité de vos correspondants.
  - Il est inutile d'envoyer à un correspondant amical ou familial, ces adresses professionnelles, le contraire est aussi vrai.
  - Une recherche sur des sites spécialisés comme www.hoaxbuster.com ou www.secuser.com/hoax, peut éviter d'être piégé.