Micro-ordinateurs – Réseaux
Protection

Auteur : C. Terrier ; mailto:webmaster@cterrier.com **;** http://www.cterrier.com

Source **:** http://www.cnil.fr/ et http://www.secuser.com/

L'utilisation de micro-ordinateurs connectés au réseau Internet impose de mettre en œuvre des protections destinées à sécuriser les données, les transferts et les postes.

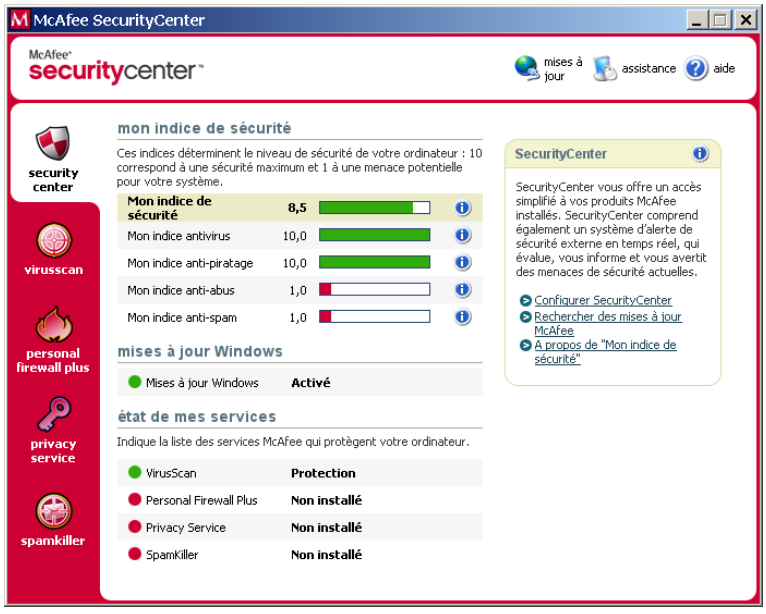
Les risques encourus sont les suivants :
1. Contamination par des virus informatiques qui peuvent détériorer des données, des programmes ou le système d'exploitation de l'ordinateur.
2. Contamination par un virus du type «Cheval de Troie» qui prend le contrôle partiel de l'ordinateur.
3. Violation des accès au réseau par des «hacker» des «cracker» ou des espions qui peuvent venir lire, copier ou altérer des données du serveur ou de postes reliés au serveur par jeux, défis, vengeance, espionnage industriel, ou commercial.

1 – Protection contre les virus

Un "virus" est un programme destiné à endommager les informations qui circulent sur l'Internet, sur un ordinateur ou un réseau. Il peut détruire des mois de travail, et créer de graves perturbations de fonctionnement.

Les virus sont introduits dans un ordinateur par un fichier contaminé enregistré sur un support informatique (disquette, clé USB, CDROM) ou par le téléchargement de fichiers sur l'Internet. Enfin il peut être contenu dans une pièce jointe d'un e-mail.

Il s'auto reproduit et infecte des programmes ou des fichiers. Il entre en action à l'ouverture du programme ou du fichier infecté puis se reproduit et infecte les autres fichiers présents sur le disque dur ou sur le réseaux.



La meilleure des protections consiste à installer sur l'ordinateur ou sur le réseau, un logiciel antivirus. Ces programmes gardent en mémoire la signature informatique de tous les virus connus. Ils scannent tous les entrées et sorties de l'ordinateur. Lorsqu'une signature est identifiée, ils proposent de détruire le fichier ou de le mettre en quarantaine. Attention : il apparaît sans cesse de nouveau virus et pour bénéficier d'une protection totale il est capital de réaliser régulièrement une mise à jour via l'Internet des nouvelles souches.

Important :
- Installer un antivirus efficace, adapté à votre ordinateur (Windows 98, 2000, XP, Mac OS.),
- Sauvegarder régulièrement vos documents,
- Prix : 40 à 60 € TTC. (Norton AntiVirus de Symantec ou McAfee de Networks Associates Technology).

2 – Protection contre les accès non désirés

Des individus malintentionnés peuvent espionner vos données ou prendre le contrôle de votre ordinateur.

- Ce risque est mineur dans le cas d'une connexion à l'Internet, car les données peuvent emprunter des chemins très différents.
- Des protocoles sécurisés sont mis en oeuvre pour les paiements en ligne (les données transmises sont cryptées ce qui permet de garantir l'intégrité et la confidentialité des données échangées entre client et serveur.

Le risque le plus sérieux est celui de l'**intrusion** dans l'ordinateur d'un programme de type « Cheval de Troie ». Ces programmes informatiques sont cachés dans un autre et exécute des commandes à votre insu. Généralement, il donne un accès à la machine sur laquelle il est exécuté en ouvrant une porte dérobée, par extension il est parfois nommé troyen par analogie avec les habitants de la ville de Troie.

- Ce risque est important si vous disposez d'une adresse IP fixe (câble, ADSL, ligne spécialisée). Car le pirate dispose alors de tout son temps pour étudier votre système et tenter d'y trouver une faille.
- Si vous disposez d'une adresse IP dynamique (qui change à chaque connexion), le risque est moindre. Mais il existe des virus dit « Cheval de Troie » qui trahissent votre adresse IP lorsque vous êtes connectés et permette à un hacker de prendre la direction de votre ordinateur pour lui faire réaliser des tâches à votre insu.

La solution consiste à installer un pare-feu (firewall) qui va surveiller les données entrantes ou sortantes, en examinant les données de contrôle. Comme la surveillance s'exerce au niveau TCP/IP, les paquets hostiles ou indésirables sont bloqués.
Il existe des firewalls simples, performants et gratuits comme **Zone Alarme**. Les paramètres par défaut assurent une protection optimale pour une utilisation personnelle. (Autres programmes : Norton, McAfee etc.)

3 – Protection des accès

Le risque de perte, vol, (portable) ou l'accès par un tiers non autorisé (espionnage industriel) à un micro-ordinateur impose la mise en œuvre des dispositifs de protection pour rendre ces évènements sans conséquence.

- Les ordinateurs peuvent être protégés au démarrage (lors de la mise sous tension) par la saisie d'un mot de passe. Attention, cette protection est contournable par un professionnel. Un mot de passe efficace compte au moins sept caractères alphanumériques. Il est changé régulièrement et ne doit pas être facile à trouver (nom du conjoint, des enfants, de l'ami(e) de l'animal de compagnie, date de naissance etc.).
- Le contrôle d'accès à un ordinateur peut être effectué par un système de biométrie (empreintes digitales) ou par une clé électronique (sur port USB). Certaines clés électroniques utilisent d'ailleurs la biométrie.
- Le paramétrage, dans le système d'exploitation, d'un identifiant (distinct du nom de l'utilisateur) et d'un mot de passe garantie une protection. Le système d'exploitation permet souvent d'administrer des «profils utilisateurs» et de limiter les accès à certains postes, disques, logiciels, dossiers et données.
- La mise en œuvre d'un écran de veille protégé par un mot de passe interdit l'utilisation du microordinateur dans le cas de sa non utilisation.

4 – Protection des données décentralisées :

- Les données du serveur, copiées sur un autre poste présentent le risque d'être périmées car non synchronisées avec celles du serveur. Ces procédures doivent être limitées et contrôlées. Il est indispensable d'envisager à chaque fois si un simple accès en consultation à distance ne suffit pas.

- Dans le cas d'enregistrement des données sur un autre ordinateur, il est obligatoire de se garantir de la non péremption de ces dernières au moment de leur utilisation. Lors de la synchronisation entre l'ordinateur et le réseau, des contrôles peuvent être effectués sur la cohérence et l'intégrité des données.