La criminalité par Internet touche la société, les individus, les organisations, les Etats, par manipulations d'opinion, espionnage, terrorisme, harcèlement, escroqueries et fraudes financières. Cependant les individus et les entreprises de toutes tailles peuvent être confrontés **au quotidien** à des **risques réels de cybercriminalité**. Il existe de multiples cas pratiques dans lesquels un simple individu ou une entreprise modeste peut être confronté à ce type de délinquance : vols de données bancaires (carte de paiement), fraudes sur l'achat en ligne, vols ou destructions d'informations numériques, divulgation d'informations sensibles, « effacement » de site Internet, chantage et extorsion, perte de disponibilité des systèmes informatiques, ... Selon une étude de la société McAfee, en 2008 les fraudes et actions cybercriminelles coûteraient près de 1000 milliards de \$ par an aux entreprises dans le monde.

Nous assistons depuis quelques années à un phénomène en pleine expansion porté par le simple fait qu'il génère des sommes d'argent de plus en plus importantes. La revente de données bancaires piratées génère un « chiffre d'affaires » proche des 7 milliards d'€ chaque année, et la découverte d'une vulnérabilité dans un système informatique se paierait de 500 à 200000 \$. Il devient donc incontournable que tout internaute soit un jour ou l'autre confronté à ce phénomène.

Si on s'attarde sur les techniques les plus communément utilisées, on ne retrouve que des pratiques assez classiques aux yeux des spécialistes : le Phishing (ou « hameçonnage ») qui se résume à un appât envoyé par @mail ou par un réseau social, le classique Malware qui tente d'infecter le poste utilisateurs (virus, vers, spyware, rootkits, botnet, ...), l'ingénierie sociale auprès des collaborateurs des entreprises pour obtenir des informations, des attaques plus directes qui tenteront d'exploiter une faille technique des postes utilisateurs, ou des attaques avec intrusions sur le système d'information global d'une entreprise. L'utilisateur et son poste reste dans la majorité des cas la cible privilégiée.

Au niveau des codes malicieux (Virus, Spyware, Trojans, Adware, Worm, ...) regroupés sous la dénomination de Malware, on assiste depuis quelques années à une mutation du phénomène : la majorité est maintenant disséminée sur le Web et non plus envoyée par e-mails, leur nombre a considérablement explosé ces dernières années, et enfin une partie importante consiste à compromettre des postes utilisateurs au profit des « botnets ». Un botnet est un ensemble de machines compromises (dites zombies), regroupées dans des réseaux et utilisées simultanément lors de certaines attaques. A partir d'une console de contrôle, un pirate peut demander à un groupe de machines distantes précédemment compromises, qui peuvent appartenir à n'importe quels individus ou entreprises, de lancer une attaque simultanée pour ainsi associer la puissance du nombre à la valeur technique de son attaque. Les botnets sont ainsi utilisés pour rendre inaccessible des sites Internet (DDoS), pour l'envoi massif de Spam ou Phishing, voire pour permettre des stockages et des téléchargements illicites. On estime que 5 000 machines devraient suffire pour bloquer n'importe quel site « classique » dans le monde. En 2007, une étude IBM estimait que 5% à 11% des machines connectées à Internet étaient infectées soit entre 32 et 71 millions.

Pourquoi de telles technologies arrivent-elle à se développer aussi rapidement voire aussi facilement ? Il existe à mon sens deux facteurs de vulnérabilités évidents qui sont le facteur humain et l'ensemble des failles techniques présentes dans les systèmes et les composantes logicielles des postes utilisateurs. L'utilisateur est à l'origine de la propagation de nombreux virus au début des années 2000, il reste une cible facile favorisant l'émergence de la cybercriminalité non seulement par un manque évident de méfiance mais aussi parce qu'il est non sensibilisé et mal informé sur les risques et leurs conséquences. Le personnel de l'entreprise doit être considéré comme un élément à sécuriser du système d'information au même titre que les moyens techniques.

Qu'en est-il des failles de sécurité ? Les failles de sécurité des systèmes d'exploitation et des composantes logicielles des postes utilisateurs restent un sujet plus d'actualité. Une vulnérabilité ou une faille technique peut se résumer à une erreur de programmation ou de conception d'un élément logiciel utilisé sur un poste. En découvrant une telle faille, un pirate va tirer profit de celle-ci en créant par exemple un outil ou une procédure d'attaque permettant de prendre le contrôle ou d'altérer le poste visé. Des failles de sécurité sont régulièrement découvertes et publiées par les éditeurs ou les spécialistes, et en général une telle découverte entraîne une mise à jour des produits affectés.

Quelles sont les mesures de protection disponibles ? Il n'existe pas de contre-mesure de sécurité générique à mettre en place. La bonne sécurité a toujours consisté pour une entreprise à établir une politique de sécurité informatique réfléchie, adaptée et suivie. Dans celle-ci apparaîtront un ensemble de contre-mesures de sécurité diverses qui associées les unes avec les autres seront efficaces.

En conclusion, la cybercriminalité est une composante quotidienne de l'insécurité informatique et doit être prise en compte dans toute réflexion portant sur la sécurité informatique. Il n'existe pas de mesure de sécurité unique, seule la mise en place d'un processus de sécurisation globale (incluant sécurité par management, sécurité logique, plan de continuité, ...) sera réellement efficace.