***Quels sont les risques ?***

***Evaluation des risques liées à l'utilisation de l'informatique***

*Il importe de mesurer ces risques :*

*— en fonction de la probabilité ou de la fréquence de leurs survenances ;*

*— en mesurant leurs effets possibles.*

*Ces effets peuvent avoir des conséquences* ***négligeables*** *ou* ***catastrophiques :***

*— le traitement informatique en cours échoue : il suffit de le relancer, éventuellement par une*

 *autre méthode si on craint que la cause ne réapparaisse ;*

*— l'incident est bloquant et on doit procéder à une réparation ou une correction avant de*

 *poursuivre le travail entrepris.*

*Mais ces mêmes incidents peuvent avoir des conséquences beaucoup plus fâcheuses :*

*—* ***données irrémédiablement perdues*** *ou* ***altérées****, ce qui les rend inexploitables ;*

*—* ***données*** *ou* ***traitements durablement indisponibles****, pouvant entraîner l'arrêt d'une*

 *production ou d'un service ;*

*—* ***divulgation d'informations confidentielles*** *ou* ***erronées*** *pouvant profiter à des sociétés*

 *concurrentes ou nuire à l'image de l'entreprise ;*

*— déclenchement d'actions pouvant provoquer des* ***accidents physiques*** *ou induire des*

***drames humains****.*

**Les risques humains**

Ce sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés.

Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

— la **maladresse** : commettre des erreurs : exécuter un traitement non souhaité, effacer

 involontairement des données ou des programmes, etc.

— **l'inconscience** et **l'ignorance** : introduire des programmes malveillants sans le savoir (par

 exemple lors de la réception de courrier).

*De nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils font courir aux systèmes qu'ils utilisent.*

Réaliser des manipulations inconsidérées (autant avec des logiciels qu'avec du matériel)

— la **malveillance** : impossible d'ignorer les différents problèmes de virus et de vers ces dernières années (beaucoup de couverture médiatique).

*Certains utilisateurs peuvent volontairement mettre en péril le système d'information, en y introduisant en connaissance de cause des virus (en connectant par exemple un ordinateur portable sur un réseau d'entreprise), ou en introduisant volontairement de mauvaises informations dans une base de données.*

*Il est facile pour un informaticien d'ajouter délibérément des fonctions cachées lui permettant, directement ou avec l'aide de complices, de détourner à son profit de l'information ou de l'argent. On parle alors de la « cyber-criminalité ».*

— **l'ingénierie sociale** (*social engineering*) est une méthode pour obtenir d'une personne des

 informations confidentielles, que l'on n'est pas normalement autorisé à obtenir, en vue de

 les exploiter à d'autres fins (publicitaires par exemple).

 Elle consiste à :

 - se faire passer pour quelqu’un que l’on est pas (en général un administrateur)

 - demander des informations personnelles (nom de connexion, mot de passe, données

 confidentielles, etc.) en inventant un quelconque prétexte (problème dans le réseau,

 modification de celui-ci, heure tardive, etc.).

 Elle peut se faire soit au moyen d’une simple communication téléphonique, soit par mail,

 soit en se déplaçant directement sur place.

— **l'espionnage** : surtout industriel, emploie les même moyens, ainsi que bien d'autres, pour

 obtenir des informations sur des activités concurrentes, procédés de fabrication, projets en

 cours, futurs produits, politique de prix, clients et prospects, etc.

 Des formes à la limite de la légalité correspondent à « **l'intelligence économique** ».

**Les risques matériels**

Ils sont liés aux défauts et pannes **inévitables** que connaissent tous les systèmes matériels et logiciels.

Ces incidents sont plus ou moins fréquents selon le soin apporté lors de la fabrication et l'application de procédures de tests effectuées avant que les ordinateurs et les programmes ne soient mis en service.

Certaines de ces pannes ont des causes indirectes, voire très indirectes, donc **difficiles à prévoir**.

— **Incidents liés** au **matériel** : la plupart des composants électroniques, produits en grandes séries, peuvent comporter des défauts. Ils finissent un jour ou l'autre par tomber en panne.

Certaines de ces pannes sont assez difficiles à déceler car **intermittentes** ou **rares**.

Parfois, elles relèvent d'une erreur de conception (*une des toutes premières générations du*

*processeur Pentium d'Intel pouvait produire, dans certaines circonstances, des erreurs de calcul*) .

— **Incidents liés** au **logiciel** : mes plus fréquents ;

Les systèmes d'exploitation et les programmes sont de plus en plus complexes car ils font de plus en plus de choses. Ils nécessitent l'effort conjoint de dizaines, de centaines, voire de milliers de programmeurs. Ces programmeurs peuvent faire des erreurs de manière individuellement ou collective que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité.

— **Incidents liés** à **l'environnement** : les machines électroniques et les réseaux de comunication sont sensibles aux variations de température ou d'humidité (tout particulièrement en cas d'incendie ou d'inondation) ainsi qu'aux champs électriques et magnétiques.

Il est possible qu'un ordinateur tombe en panne de manière définitive ou intermittente à cause de conditions climatiques inhabituelles ou par l'influence d'installations électriques notamment industrielles (et parfois celle des ordinateurs eux-mêmes !).

**Les précautions à prendre**

Dans le cas des risques matériels il est possible de se prémunir :

— **redondance des matériels** : la probabilité ou la fréquence de pannes d'un équipement est

représentée par un nombre très faible (compris entre 0 et 1, exprimé sous la forme 10^-n).

En doublant ou en triplant (ou plus) un équipement, on divise le risque total par la probabilité de pannes simultanées.

Le résultat est donc un nombre **beaucoup plus faible** et la fiabilité est plus grande.

— **dispersion des sites** : un accident (incendie, tempête, tremblement de terre, attentat, etc.) a très peu de chance de se produire simultanément en plusieurs endroits distants.

— **procédures** de **contrôle indépendants** : ils permettent bien souvent de déceler les anomalies avant qu'elles ne produisent des effets dévastateurs.

Il est possible de réaliser des **audits** de sécurité.

**Sécurité et Sureté**

On parle de :

— « **Sécurité** de fonctionnement » dans le cas de la protection des données et de la capacité de travail

contre les actes de malveillance ;

— « **Sureté** de fonctionnement » dans le cas de la protection du système d'information contre

 les accidents

**Les programmes malveillants**

Un logiciel malveillant (malware en anglais) 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 d'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.

— **l'exploit** : programme permettant d'exploiter une faille de sécurité d'un logiciel ;

— le **rootkit** : ensemble de logiciels permettant généralement d'obtenir les droits d'administrateur sur une machine, d'installer une porte dérobée, de truquer les informations susceptibles de révéler la compromission, et d'effacer les traces laissées par l'opération dans les journaux système.