Chapitre 01 : Sécurité Informatique

1. Concepts de base

Définition de la sécurité informatique : l'ensemble de ***moyens*** mis en œuvre pour ***minimiser*** la ***vulnérabilité*** d'un système contre les ***menaces accidentelles*** ou ***intentionnelles***.

La sécurité informatique est un domaine ***pluridisciplinaire*** parce qu'il englobe des moyens ***techniques***, ***juridiques***, ***humaines*** et ***organisationnels***. Il semble évident que la sécurité informatique commence par la sécurité de l'environnement physique dans lequel le système informatique est installé (par exemple, les salles des serveurs) contre les accès non-autorisés. En plus, nous devons sécuriser les systèmes informatiques contre les accidents (comme les inondations et les feux). La boite noire d'un avion est un exemple typique de ce cas. En fait, le contenu de ces systèmes informatiques (les boites noires) est protégé contre les dommages provoqués par les accidents des avions.

Naturellement, l'aspect **humain** prend une partie importante dans la sécurité informatique. C'est l'être humain qui conçoit, implémente et utilise les systèmes informatiques. Sachant que l'erreur est humaine, ces dernières peuvent engendrer des résultats catastrophiques. Il est possible aussi d'exploiter les failles humaines et sociales pour l'exploitation déloyale de l'information. Nous parlons dans ce cas de **l'ingénierie sociale (Social Engineering)**. On peut, à titre indicatif, noter que 85% de détournement sont réalisés sans ordinateur. En fait, si Ramy Badir a estimé qu'un ordinateur sécurisé est un ordinateur entreposé dans un hangar et débranché, Kévin Mitnick (qui a popularisé le concept de l'ingénierie social) a signalé qu'on peut toujours trouver quelqu'un qui branche un ordinateur (c'est-à-dire il a noté qu'on peut manipuler les utilisateurs ignorant durant pour menacer des systèmes informatiques).

Dans une organisation, l'aspect **organisationnel** est un aspect essentiel de la sécurité informatique. En effet, la politique de la sécurité informatique est spécifiée à ce niveau. En étudiant les besoins de l'organisation et les la vulnérabilité d'un système informatique, nous pourrons identifier les actions autorisées et les actions interdites durant la manipulation d'un système informatique.

Bien entendu, la sécurité informatique n'a pas de sens sans un cadre **juridique** permettant la définition des crimes informatiques et leurs sanctions. Il est connu en sciences juridiques qu'il n'y a pas de peine sans loi. Ainsi, l'apparition des crimes informatiques dans la société nécessite la mise à jour des lois afin d'introduire ces nouvelles crimes.

Il est important de noter que la définition précédente de la sécurité informatique n'exige pas **d'éliminer la vulnérabilité** d'un système mais juste de la **minimiser**. En fait en plus de la difficulté technique (voir l'impossibilité) d'éliminer cette vulnérabilité, le **coût** d'une telle tentative peut être au-delà de dommages possibles d'une menace.

La vulnérabilité est définit comme une faute accidentelle ou intentionnelle introduite dans la spécification, conception ou la configuration d'un système et qui peut être exploité pour créer une intrusion.

Un attaque est une faute d'interaction malveillante vise à violer une ou plusieurs attributs de la sécurité informatique.

Il est important de noter que les menaces ne consistent pas seulement à l'accès direct aux données. Plusieurs actions peuvent être considérées comme des menaces malgré que l'analyse rapide puisse les considérer comme des actions autorisées. Par exemple, l'analyse de trafic dans un réseau est un acte autorisé (surtout dans le cas de recensement et statistiques). Cependant, il est possible de déduire certaines informations secrètes à partir de l'analyse des informations échangées. Par exemple, les échanges entre les corps militaires durant la préparation des attaques peut être sont plus dynamiques par rapport aux échanges dans le cas normal.

Ces menaces peuvent aussi prendre la forme d'inférence. Dans ce cas, il est possible de déduire des données secrètes à partir de données indiscrètes.

2. Types de menaces

On peut classifier les menaces selon plusieurs critères :

2.1. **Selon l'acteur :** nous distinguons généralement deux types de menaces selon ce critère : interne et externe. En fait, une menace peut être engendré par un acteur au sein de l'organisation (de manière intentionnelle ou accidentelle)

comme elle peut être engendré par un acteur externe de l'organisation. Il est important de prendre ce critère en considération lors la gestion de la sécurité informatique. L'ignorance de ce critère a créé une situation paradoxale. En effet, malgré que 80% de menaces sont d'origine d'un acteur interne, on remarque que 80% à 90% de budget consacré à la sécurité est destiné à traiter les menaces d'origine externe.

2.2. **Selon le mode :** on distingue selon ce critère les menaces intentionnelles et les menaces accidentelles. Les menaces intentionnelles sont exécutées avec l'objectif de endommager le système informatique. Par contre, des menaces accidentelles sont dues à des accidents environnementaux ou opérationnels. Les feux, les inondations et les pertes de données à cause de fausses manipulation sont des exemples de cette catégorie. On distingue deux sous catégories de menaces intentionnelles : des menaces passives et des menaces actives. Dans les menaces passives on ne change pas les données et les programmes de système informatique mais l'objectif est de consulter des données qu'on n'a pas le droit à les consulter. Les menaces actives ciblent le changement de données ou des programmes.

2.3. **Selon la vulnérabilité :** le dernier critère qu'on peut l'utiliser pour classifier les menaces est la vulnérabilité. En fait, on peut distinguer les menaces selon le point vulnérable exploité pour attaquer le système. Ainsi, nous pouvons distinguer deux sous critères : la nature du point vulnérable ou la phase dans laquelle l'erreur a été introduite. Un système informatique est composé de plusieurs entités différentes comme des logiciels (système d'exploitation, protocoles de communication, logiciels d'application) ou matériels (hardware, des disques de stockages, des câbles réseaux). Chaque entité de ces dernières peut être exploitée pour attaquer un système informatique. Bien entendu, la protection d'un matériel informatique est différente de la protection des logiciels. En plus, la protection des chaque type des logiciels ou matériels est différente de la protection des autres types. Ainsi, il est important de distinguer les menaces selon le point faible exploité. En plus, chaque entité est crée (développée ou fabriquée) en suivant un ensemble de phase qui consistent généralement en spécification, conception, développement et configuration. Le point vulnérable est une faute comme nous avons mentionné auparavant. Cette faute peut être engendrée dans n'importe quelle

étape des étapes précédentes. En conséquence, nous pouvons distinguer les menaces selon la phase dans laquelle le point vulnérable a été commis. Cette classification, nous permet de mieux diagnostiquer le problème afin de proposer des solutions efficaces.

3. Les attributs de la sécurité informatique

La sécurité informatique est un domaine vaste considérant les techniques utilisées, les cibles à protéger et acteurs intervenant. Cependant, il existe certains objectifs qu'on cherche à satisfaire dans la plupart des cas de la sécurité informatique. Ces objectifs, appelés aussi des attributs de la sécurité ou des services de la sécurité, ne sont pas au-delà de débats. A notre avis, les principaux attributs de la sécurité informatique sont :

3.1. La confidentialité : qui consiste à protéger les informations de lecture non-autorisée ;

3.2. L'intégrité : c'est-à-dire un tiers ne peut pas changer ou détruire les informations qui existent dans un ordinateur ou qui traversent un réseau. Au pire de cas, l'utilisateur de système informatique peut détecter le changement de ces informations.

3.3. Disponibilité : cet attribut signifie que les gens autorisés à l'utilisation d'un système informatique ne seront pas empêché de le faire.

3.4. No-répudiation : Cela signifie que quelqu'un qui a manipulé le système informatique, ne peut pas dénier de cet acte.