**Chapitre 1 :** Introduction à la sécurité Informatique

1. **Définition**

**Sécurité Informatique** : C’est l'ensemble des moyens mises en œuvre pour protéger un bien.

**La Cybersécurité** : C'est l'ensemble des moyens mises en jeu pour protéger un bien dans un réseau cybernétique.

**NB :** Cybernétique =ouvert aux publics

**Menace** : c’est une cause potentielle d'incident qui peut engendrer un dommage dans un système.

On distingue 02 types de menaces : menace interne (volontaire ou involontaire) et menace externe (fait allusion au différents types de menaces).

**Vulnérabilité** : c’est une faille sur un système informatique pouvant servir de moyen aux criminels de porter atteinte à la sécurité de ce système.

**Attaque** : c’est l'exploitation des failles d'un système pour porter atteinte à sa sécurité //toute tentative d'intrusions dans un système non autorisé

**Donnée** : c’est la représentation d'une information sous forme conventionnelle.

NB : les données se présentent sur 3 formes dont :

* **Au repos**
* **En cours de traitement**
* **En transmission**

**Politique de Sécurité** : c’est un document rédigé par le système de pilotage qui définit comment la sécurité sera planifier, exécuter, maitriser.

**Gestion de la sécurité** : c’est l'application des connaissances, des compétences, des outils et techniques aux activités de la sécurité informatique pour satisfaire les exigences.

**Infraction** : c’est une violation d'une ou de plusieurs règles de sécurité. Il en existe 3 types :

* **Les infractions spécifiques aux technologies de l'information et de la communication**
* **Les infractions liées aux technologies de l'information et de la communication**
* **Les infractions facilitées par les technologies de l'information et de la communication**

1. **Notion de CID(DIC)(Confidentialité Intégrité et Disponibilité)**
2. **Confidentialité**

Consiste à empêcher la divulgation des informations à des personnes ou des ressources des processus non autorisés. Un autre terme pour cela est la vie privée, pour mettre en place ce principe dans un système informatique :

* Les organisations doivent former leurs employés aux meilleurs pratiques en matière de protection des informations sensibles afin de se protéger et protéger les entreprises des attaques
* les méthodes utilisées pour assurer la confidentialité incluent le cryptage ,l'authentification et le contrôle d'accès (informations sur des personnes, les informations relatives à l'activité de l'entreprise, les informations classifiées (ceux-ci concernent les informations sensibles vu qu'il existe

Deux types informations dont sensibles et insensibles))

1. **Contrôle d'accès**

Le Contrôle d'accès désigne les différentes solutions et méthodes visant à gérer l'accès à une ressource, il existe deux types de contrôle d'accès : **les contrôles d'accès physiques et les contrôles d'accès logiques.**

* **Le contrôle d'accès physiques** : vise à limiter tout accès de l'utilisateur aux ressources (ce qui peut se faire en créant des salle serveurs, des data center éloigner de l’organisation, bloquer les ports USB des machines)
* **Le contrôle d'accès logique :** vise à restreindre l'accès au **réseau informatique** (exemple : **le filtrage des communications** (comme outils nous avons **: portail captif, ACL, proxy, pare feu**), définir les niveaux d’accès), aux **données** (exemple : **définition des rôles**, stratégies de groupe, définition des droits d’accés, des profils) à un système informatique

1. **L’authentification**

C'est un mécanisme qui consiste à vérifier les informations d'identification d'une ressource afin de lui donner accès au système. Il existe 4 méthodes d'authentification courante notamment :

* **L’authentification par mot de passe** qui consiste à attribuer à chaque acteur du système un nom d'utilisateur et un mot de passe comme information d'identification cette authentification est basée sur le principe de « **ce que je connais »**
* **L’authentification par carte**, dans cette méthode les informations d'identification sont placées dans une carte et est remis à l'acteur du système qui l'utilisera pour s'identifier dans le système, cette méthode est basée sur la politique de « **ce que j'ai** »
* **L'authentification biométrique** qui utilise les moyens biologiques (l’œil, le nez, l’empreinte, l’ADN,) comme support d'identification dans un système, cette méthode utilise la politique de « **ce que je suis »**
* **Identification par** **TOKEN** qui utilise un support notamment clé USB comme moyen d’identification, cette méthode est basée sur la politique de « **ce que j'ai »**

Pour garantir l'authenticité d'une information on effectue : **un chiffrage** qui consiste à transformer un texte clair en un illisible), il existe deux types de chiffrement :

* **Le chiffrement symétrique** comme avantage : **Rapidité d’exécution, simple à mettre en œuvre** ; inconvénient on peut intercepter la clé de chiffrement lors de l'envoi du message, **moins fiable**, on utilise une **même clé pour chiffrer et pour déchiffrer**
* **Le chiffrement asymétrique** on utilise une clé pour chiffrer et une autre pour déchiffrer. **Fonctionnement**: génération des clés et partage ,chiffrage du message avec les clés publiques et ils sont déchiffrés avec les clés privées ;PKI(Infrastructures de clés à Privées, modèle d'application autorité de certificat ,les blockchaine) qui sont des infrastructures dans lesquelles on retrouve des chiffrements symétrique et asymétrique ,qui est l'ensemble des données matériels et logiciels misent ensemble pour garantir **l'authentification, l’intégrité ,la confidentialité, le non répudiation** dans un système informatique.

b.1) **Chiffrement Symétrique**

**Le chiffrement de César**

Exemple : abcdefghijqlmnopqrstuvwxyzabc (message normale)

Clé = 3 abcdefghijklmnopqrstuvwxyz

Tirer=qfobo

**Le chiffrement de vigenére (voir cahier)**

**b. 2) filtrage**

* Installer un serveur proxy pour gérer l'accès au ressource. Les règles de filtrage sont fixées au niveau du proxy
* Utilisation d'un pare-feu tous en sachant que les attaques peuvent venir de l'intérieur l'on peut avoir deux pare feu et compris ainsi la dmz
* Authentification Forte :

Méthode Courante d'Authentification :

* **Otp (On time Password)** : qui consiste à changer son mot de passe durant un temps
* **SSO** : ici si on se connecte sur une application on aura plus besoin de le faire sur une autre application car il lira tout simplement le fichier concernant ce mot de passe, aussi il améliore la sécurité dans le sens où l'utilisateur ne devra plus fournir des efforts en terme de réflexion
* **PKI**

1. **Intégrité**

Consiste à garantir la précision, la cohérence, et la fiabilité d’une ressource durant son cycle de vie. Les méthodes utilisées pour garantir l’intégrité d'une ressource sont :

* **Le hachage**
* **Signature numérique**
* **Certificat numérique**

**NB : Le contrôle de validation pour valider que la ressource initialement prévu est toujours là même, Le contrôle de cohérence, Le contrôle d'accès : qui sont des propriétés des fonctions qui doivent remplir l’intégrité**

1. **Disponibilité**

C'est la capacité qu'a un bien à être accessible par une ressource autorisée au moment voulu. Elle peut être appliquer dans les domaines suivants **:**

* **Finance**
* **Santé**
* **Nucléaire**
* **Aéronautique.**

**La haute disponibilité** désigne la capacité qu'à un système a respecté **la règle des 5 neuf (99.999%)** soit la capacité d'être disponible **à 99.999,** pour gérer ainsi cela on met sur pied des méthodes telles que : **PCA (plan de continuité d’activité) /PRA (plan de reprise d'activité),** la différence entre ces deux méthodes est que :

* **Le PCA :** comme moyens on peut avoir :
* **La sauvegarde**
* **La redondance :** qui consiste à dupliquer les données sur des supports différents, qui intègre ainsi l**a réplication, la factorisation)**
* **La virtualisation** dont les types sont : **paas, software(Saas)iaas**
* **L’isolation (**qui consiste à séparer l'opérationnel des services**)** c'est un concept qui consiste à faire une abstraction de la réalité, met en placeun ensemble de processus dans le but de favoriser la continuité d'une activité
* **Le PRA** met en place un ensemble de processus dans le but de favoriser la reprise d'une activité.

**NB : la sauvegarde** est l'opération qui consiste à copier les données d'une source principale vers une source secondaire**, la réplication** est différent de la sauvegarde**,** il existe 3 types d'infrastructures dont **: on promise (sur les lieux), virtuelle, hybride**

**RQ**:1 ere dimension concerne les objectifs de sécurité qui sont : **Confidentialité, Intégrité, Disponibilité**

**2 iémé dimension** on identfit les biens sur lesquelles on va appliquer ces objectifs de sécurité qui **est : les données (**qui se présente sous trois formes **repos, transiste, traitement)**

**3iéme dimension** les moyens pour pouvoir atteindre les objectifs**: les technologies, procédures, les processus les lois, humains,**

**Nb :**