Qu’est-ce que la sécurité informatique ?

La sécurité informatique est l’ensemble des méthodes permettant de protéger les données et les systèmes permettant de véhiculer, de stocker ces données.

Quels les composantes de la sécurité informatique

La sécurité est essentielle pour la protection de trois caractéristiques des systèmes et de l’information qu’ils traitent et maintiennent à savoir,

- Sa confidentialité qui assure que l’information soit protégée contre tout divulgation accidentelle ou malveillante.
- L’intégrité qui assure les données et les systèmes soient protégés contre toutes modifications ou destructions accidentelle ou malveillante.
- La disponibilité qui assure que l’information et les systèmes soient accessible et utilisable par les parties autorise aux moments où ils en ont besoin.

Qui sont les pirates informatiques ?

Un système d’information n’est pas un coffre-fort blinde : il est forcément interconnecté avec d’autres systèmes d’où le risque qu’ils soient expose à des vols de données ou d’intrusion par des gens, malintentionnés appelé pirates.

Cependant les pirates informatiques ont des motifs et des objectifs différents et varies. Ceux qui nous permet des classes dans différents groupe à savoir : les hackers, les crackers, les saboteurs, les fraudeurs et arnaqueurs et les espions.

Quels sont les menaces, vulnérabilités et risques ?

L’expert en sécurité informatique doit connaitre son système afin de pouvoir prévenir les menaces et les risques lors d’une attaque mais surtout sa vulnérabilité.

Dans le domaine de l’informatique, la menace peut se traduire comme l’action ou l’événement dont le déclenchement pourrait porter atteinte a l’une voire a plusieurs des caractéristiques critique de l’information et des systèmes qui la traitent et la maintiennent à savoir la confidentialité, l’intégrité et la disponibilité.

On distingue deux grandes classes d’évènement ou action ou menaces a savoir :

- Les actes malicieux, calculé, volontaire tels que le piratage, l’espionnage, le sabotage qu’il soit interne ou externe. On y trouve aussi les intrusion ou accès non-autorise, les usurpations d’identité la construction et l’insertion de codes cachés, l’extraction des données, les chevaux de Troie…
- Les actes ou évènements involontaire, les accidents, les mauvaises manipulations, les oublis de sauvegardes, les bugs…

En effet toutes ces menaces pourraient être classes suivant »

- La divulgation des données
- Destructions des données

- Atteinte a l'intégrité des données
- Perte de services
- Usurpation d'identité

Qu'est-ce que la vulnérabilité

<<l'essence même de la sécurité est d'identifier et réduire la présence de vulnérabilité.>>

La vulnérabilité peut se définir comme étant le réactif qui permet a la menace de s'exécuter.

Nous pouvons distinguer deux types de vulnérabilité a savoir l'absence ou manque des procédures organisationnelles, absence ou manque de procédures et/ou mesures techniques.

@book université de Ziguinchor bibliothèque AUTHOR=Didier GODART, TITLE=sécurité informatique risques, stratégies et solutions, PUBLISHER= éditions des CCI de Wallonie s.a, YEAR=2005, ISBN=2-930287-21-7

@book université de Ziguinchor bibliothèque AUTHOR=Onisep, TITLE=les métiers de l'informatique YEAR=2014, ISBN=978-2-273-01187-7