Module Sécurité Informatique (F332)

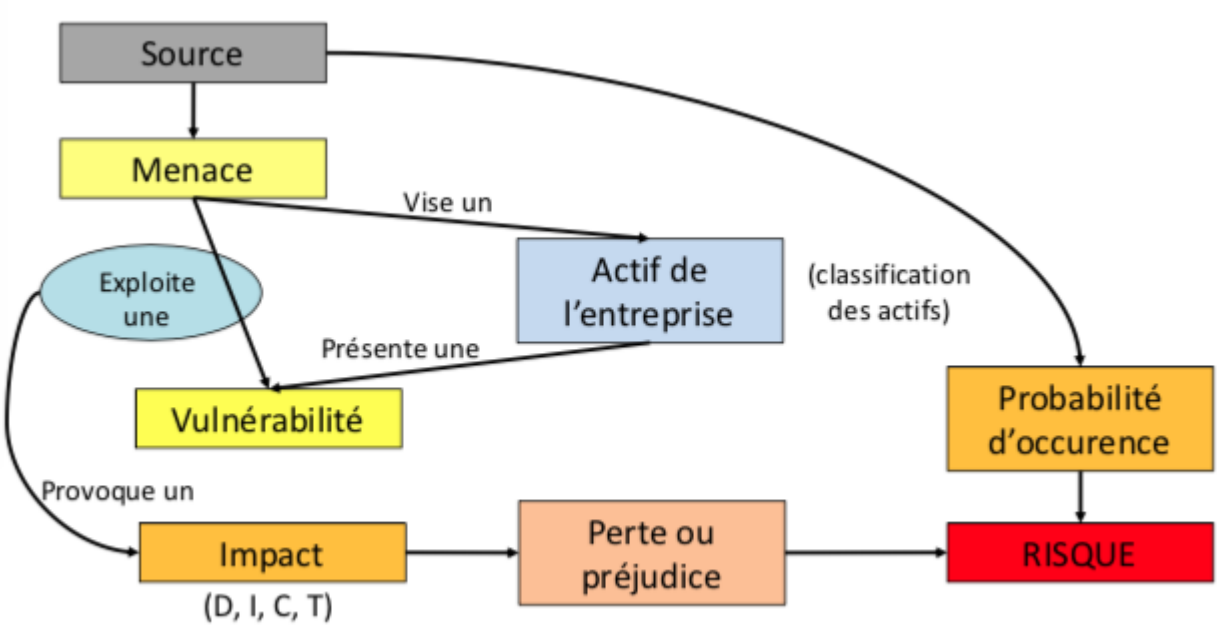
Cours 4- Gestion de Risques

Notion de risque informatique

RISQUE : Un risque est un scénario qui décrit comment des sources de risques (menaces) pourraient exploiter les vulnérabilités des systèmes jusqu'à provoquer un incident sur les éléments à protéger et causer des préjudices à l'entreprise.

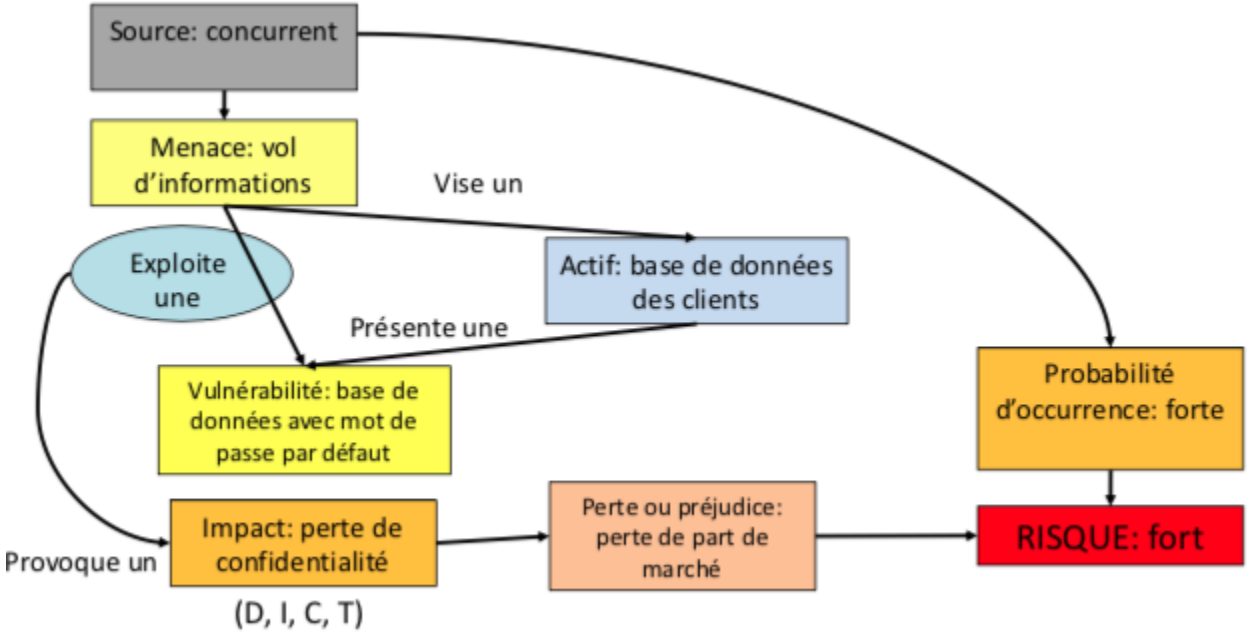
Notion de risque informatique

Schéma caractérisant le risque informatique



Notion de risque informatique

Exemple de risque informatique



Catégories de risques

Les risques sont classés en quatre grandes catégories:

1. Vol d’informations,
2. Usurpation d’identité,
3. Intrusions et utilisation de ressources systèmes,
4. Mise hors service des systèmes et ressources informatiques.

Conséquences des risques

- Une perte d’information et de données,
- Une perte d’image,
- Une perte financière
- …

Gestion de risque informatique

Gestion de risque: La gestion des risques est la mise en place de stratégies, processus, méthodes et outils destinés à faire face aux risques.

Processus de gestion de risque informatique

Le processus de gestion de risque comprend:

- Identification des risques
- Évaluation des risques
- Traitement des risques

Processus de gestion de risque informatique

Identification des risques: cette étape consiste à identifier les menaces et les vulnérabilités présentes au sein du système

Processus de gestion de risque informatique

Évaluation de risque:

Deux critères sont retenus pour « peser » le risque :

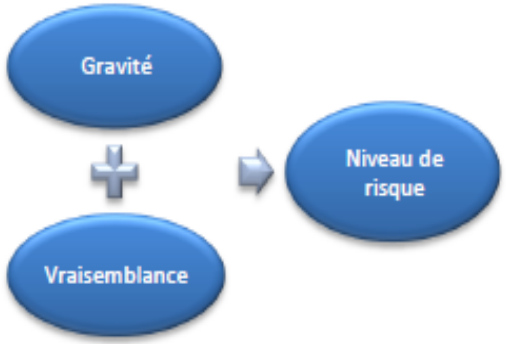
– La Probabilité (vraisemblance) de survenance

– L’impact en cas de survenance (gravité)

Niveau de risque informatique

Le **niveau d'un risque** est estimé en termes de gravité et de vraisemblance.

La gravité représente l'ampleur d'un risque.
Elle dépend essentiellement du caractère préjudiciable des impacts potentiels.



La **vraisemblance** traduit la faisabilité d'un risque.
Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

Risque= Gravité X Vraisemblance

Traitement des risques informatiques

Le traitement des risques informatiques consiste à mettre en place les contre-mesures permettant de minimiser l’exposition aux risques

Matrice d’évaluation de risques

Une matrice d’évaluation des risques est un outil qui permet de calculer le niveau de criticité d’un risque.

Les deux paramètres principaux de la criticité sont la probabilité d'apparition (vraisemblance) et la gravité. On donne en général quatre à cinq niveaux à chaque paramètres :

Vraisemblance:

1. Très improbable.
2. Improbable (rare).
3. Probable (occasionnel).
4. Très probable (fréquent).

Gravité

1. Faible.
2. Moyenne.
3. Grave.
4. Très grave.

Matrice d’évaluation de risques

Plutôt que de multiplier les deux valeurs, on construit une matrice et ce sont les zones de la matrice qui indiquent la criticité

Exemple: