UNIVERSITE BATNA 2
DEPARTEMENT INFORMATIQUE
LICENCE 3 ISIL
Sécurité Informatique

CHAPITRE 2 : Menaces et vulnérabilités des systèmes d'information

Détruire, altérer, accéder à des données sensibles dans le but de les modifier ou de nuire au bon fonctionnement:

- Les motivations sont diverses et fonction de la nature des informations recherchées et de l'organisme visé.

- L'environnement lié aux technologies de l'information et de la communication est la cible de nombreuses menaces.

L'ouverture des réseaux et leur complexité croissante

Acteurs aux multiples profils

Renforcent la vulnérabilité des systèmes d'information.

UN PEU D'HISTORIQUE

- **Le *phone phreaking (1970)***
  - C'est grâce à un sifflet trouvé dans une boîte de céréales que John Draper s'est rendu célèbre.
  - Il a piraté les lignes téléphoniques de la compagnie AT&T au début des années 1970.

- ***Le premier ver informatique /Robert Tappan Morris (1988)***
  - près de 6 000 ordinateurs infectés un peu partout dans le monde, à la manière d'une maladie contagieuse

- Vladimir Levin (1994)
  - premier cyber pirate parvenu à s'introduire dans la base de données d'un établissement financier pour détourner des fonds.
- Un virus destructeur / David L. Smith (1999)
  - L'étendue des dommages qu'il a causé ont été estimés à 400 millions de dollars.
- Créé par l'Australien Julian Assange, le site Wikileaks s'est lui spécialisé dans le piratage de documents classifiés.
- En 2007, La première cyberattaque recensée visant une structure étatique durant plusieurs semaines, a émané de sites russes contre des sites de l'administration estonienne, ainsi que ceux de banques et de journaux de ce pays.

- L'année 2020 a été marquée par un grand nombre de cyber-attaques importantes et qui a quadruplé depuis le début de la crise sanitaire.

Risques, menaces et vulnérabilités

Le risque encouru par un système est lié de manière étroite à la menace et à la vulnérabilité qui le touchent, mais également aux contre-mesures mises en œuvre

➢ Origine des risques

En termes de sécurité informatique les menaces peuvent être le résultat de diverses actions en provenance de plusieurs origines :

- Causes humaines
- Causes extérieures
- Causes techniques

1- Causes humaines

- La maladresse
- L'inconscience
- La malveillance
- L'ingénierie sociale (social engineering)
- l'espionnage

La majeure partie des menaces est due à l'erreur ou la négligence humaine (utilisateurs comme informaticiens). Il ne faut pas les ignorer ou les minimiser.

2- Causes extérieures

- Sinistres
- Problèmes électriques
- Malveillance ou mauvaise manipulation

3- Causes techniques

- Incidents liés au matériel
  - Surchauffe
  - Usure
  - Défauts de fabrication
- Incidents liés au logiciel
- Programme malveillant

Vulnérabilités des systèmes d'information

- la vulnérabilité des infrastructures implique la vulnérabilité des systèmes d'information
- l'ouverture vers l'extérieur, l'interconnexion des réseaux

  - connections par voie filaire ou hertzienne, à distance, la mobilité des liaisons

  - la miniaturisation des ordinateurs et des supports d'information

un environnement plus propice encore aux attaques

Vulnérabilités SI

- **Les vulnérabilités techniques**
- **Les vulnérabilités applicatives**
- **Les vulnérabilités humaines**
- **Les organisations sources de vulnérabilités**

1- Vulnérabilités techniques

- Les bugs dans les programmes courants et les systèmes d'exploitation
- La menace des périphériques externes

2- Vulnérabilités applicatives

- Les installations par défaut
- Les mauvaises configurations

3- Vulnérabilités humaines

- Méconnaissance de la menace
- Mauvais climat social
- Insouciance
- Utilisation mal contrôlée

4- Les organisations sources de vulnérabilités

- Une organisation trop permissive et insuffisamment structurée
- L'externalisation favorise les vulnérabilités
- sous-traitants ou prestataires de services

Les contre-mesures

Dans un contexte global, la sécurité doit être assurée:

- au niveau utilisateur
- au niveau des technologies utilisées
- au niveau des données en elles-mêmes
- au niveau physique (accès à l'infrastructure)

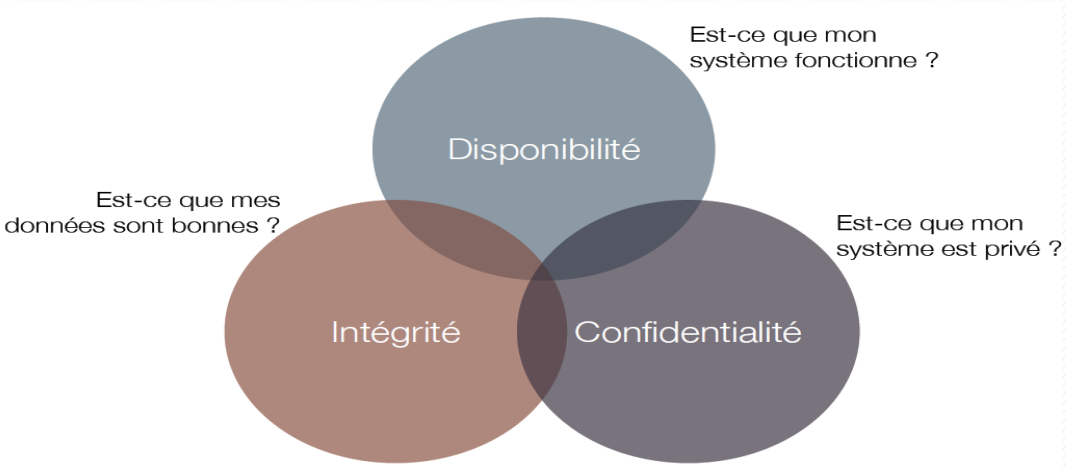
Les objectifs de la sécurité

- La sécurité n'a de sens que par rapport à ce qu'on cherche à protéger:
  - la cible principale est ***l'information***, qu'il s'agisse de la manipuler ou de la détruire, de l'extraire ou d'en restreindre l'accès, voire de la rendre inaccessible.
  - La SSI a donc pour objet de proposer des solutions organisationnelles et/ou techniques susceptibles de protéger les informations les plus sensibles en priorité mais également les autres.

Les objectifs de la sécurité

La sécurité des systèmes d'information vise généralement six ***objectifs*** :

- **Confidentialité :** garantir que seules les personnes autorisées peuvent avoir accès aux données et aux ressources de l'entreprise.
- **Intégrité :** garantir que les données échangées sont exactes et complètes.
- **Disponibilité :** garantir qu'une ressource sera accessible au moment précis où quelqu'un (entité autorisée) souhaitera s'en servir (soit 24h/24, soit aux heures ouvrables, etc.).



Les objectifs de la sécurité

- **Authentification:** a pour but de vérifier qu'une entité est bien celle qu'elle prétend être .
- **Traçabilité:** garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
- **Non-répudiation**: est le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu.

Sécurité (totale ?...) =
situation dans laquelle quelqu'un ou quelque chose n'est exposé à aucun danger, à aucun risque, en particulier d'agression physique, d'accidents, de vols ou de détériorations

Sécurité =
absence ou limitation des risques dans un domaine précis

La sécurité absolue n'existe pas.

Il faut viser un « niveau de risque acceptable ».