CH1: introduction à la sécurité

- Un système d'informations(SI) : est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.
- La sécurité des systèmes d'information(SSI): est l'ensemble des moyens nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité de l'information, des systèmes et ressources informatiques contre les menaces atteignant leur confidentialité, intégrité, et disponibilité.
- Finalités :
    - **Court terme:** chacun (légitime)ait accès aux informations dont il a besoin
    - **Moyen terme:** la cohérence de l'ensemble du système d'information.
    - **Long terme:** maintenir la confiance des utilisateurs et des clients (image de marque)
- La pluridisciplinarité de la sécurité:
    - Etique
    - Législation et réglementation
    - Technique
    - Méthodologie
    - Normes
- Objectifs de la sécurité:
    - **La disponibilité:** Le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
    - **L'intégrité:** les éléments considérés doivent être exacts et complets.
    - **La confidentialité:** Seules les personnes autorisées ont accès aux informations qui leur sont destinées.
    - **L'authentification**: L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents.
    - **La traçabilité (ou Preuve):** garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
    - **La non-répudiation:** Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées
- Risques / Menaces / Vulnérabilité:
    - **Menace** : attaque possible d'un individu ou d'un élément naturel sur des biens entraînant des conséquences potentielles négatives.
    - **Vulnérabilité**: caractéristique d'une entité qui peut constituer une faiblesse ou une faille au regard de la sécurité de l'information. Elle peut être:
        - organisationnelles
        - humaine
        - logicielles ou matérielles
    - **Impact**: conséquence sur l'organisme de la réalisation d'une menace.
    - **Risque**: la potentialité de l'exploitation de vulnérabilité par un élément menaçant et de l'impact sur l'organisme.
- Démarche générale:
    - évaluer les risques et leur criticité
    - rechercher et sélectionner les parades
    - mettre en œuvre les protections et vérifier leur efficacité.
- Approche Globale: il faut prendre en compte les aspects suivants:

- La sensibilisation des utilisateurs aux problèmes de sécurité
- La sécurité logique.
- La sécurité des télécommunications
- La sécurité physique

- La notion de politique de sécurité (PSSI): est un plan d'actions définies pour maintenir un certain niveau de sécurité et se matérialise par un ensemble de documents.
- Les normes et standards: les plus utilisés :
  - **ISO 27000:** pour la mise en place, l'utilisation, la tenue à jour et la gestion d'une politique de sécurité informatique, de sécurité des systèmes d'information ou SGSI (ISMS) : Système de gestion de la sécurité de l'information.
  - **ISO 27002:** décrit une approche processus pour la mise en place d'un SMSI (système de management de la sécurité du système d'information)
  - **ISO 27001:** Un projet de mise en place de la sécurité des systèmes d'information suit la logique de la **roue de Deming:**
    - *phase PLAN:* revient à fixer les objectifs
    - *phase DO.*
    - *la phase CHECK*: mettre en place des moyens de contrôle.
    - *phase ACT*: permettra de mener des actions correctives, préventives et d'amélioration.

CH2: La gestion des risques Concepts et méthodes

- La gestion des risques est définie par l'ISO comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque.
- Finalités:
  - Améliorer la sécurisation des systèmes d'information.
  - Justifier le budget alloué à la sécurisation du système d'information.
  - Prouver la crédibilité du système d'information à l'aide des analyses effectuées.
- Fondements: La gestion des risques se compose de trois blocs interdépendants:
  - **l'organisation en question(ses assets et ses objectifs de sécurité):**
    - *Les Assets:* biens, actifs, ressources ayant de la valeur pour l'organisme et nécessaires à son bon fonctionnement
    - *Asset business:* principalement des informations et des processus.
    - *Asset system:* les éléments techniques mais aussi l'environnement du système informatique.
  - **les risques pesant sur ces assets:**
    - *Les risques:* l'équation du risque:

      RISQUE = MENACE * VULNÉRABILITÉ * IMPACT

      → La menace: l'agent responsable du risque

→ La vulnérabilité : la caractéristique d'un asset constituant une faiblesse ou une faille au regard de la sécurité

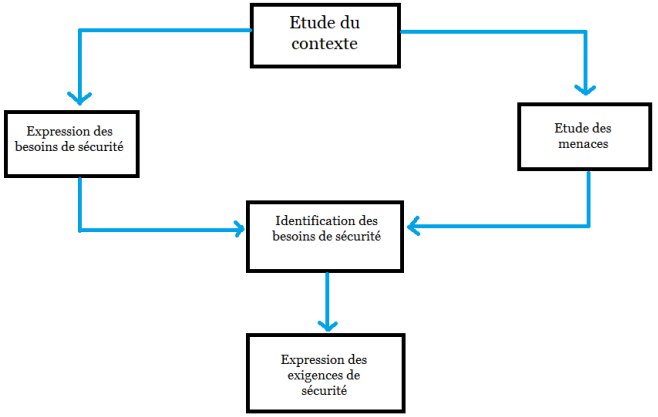
→ L'impact: la conséquence du risque sur l'organisme et ses objectifs

- **les mesures prises ayant pour but de traiter les risques et donc d'assurer un certain niveau de sécurité:** Les mesures de sécurité à mettre en place dépendent de l'activité, de l'organisation et de la réglementation ainsi que des contraintes de l'écosystème de l'entreprise.
  - *Politique de traitement de risques:* constituée d'exigences de sécurité permettant de répondre aux risques

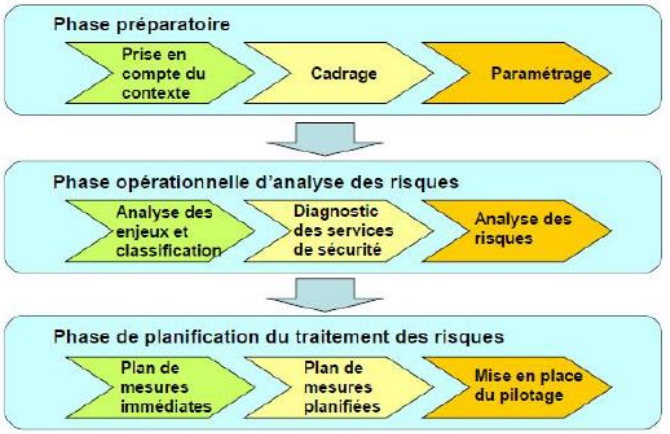
- Le processus de gestion des risques:

1. **Identification du contexte et des assets**
2. **Détermination des objectifs de sécurité:** spécifier les besoins en termes de confidentialité, intégrité et disponibilité des assets
3. **Analyse des risque:**
   - Les risques ayant une occurrence et un impact faible sont négligeables
   - Les risques ayant une forte occurrence et un impact important ne doivent pas exister
   - Les risques ayant une occurrence forte et un impact faible sont acceptés
   - Les risques ayant une occurrence faible et un impact lourd sont à transférer
   - les autres risques, en général majoritaires, sont traités au cas par cas et sont au centre du processus de gestion des risques
4. **Définition des exigences de sécurité**: est souvent effectuée de manière incrémentale et par raffinement successif
5. **Sélection des contrôles:** Les contrôles sont l'instanciation des exigences de bas niveau pour le système cible étudié
6. **Implémentation des contrôles**:

- Les méthodes de gestion des risques: Les plus connues
  - **EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)**



  - **MEHARI (Méthode Harmonisée d'Analyse de RIsques)**



  - **MARION (Méthodologie d'Analyse et de Réduction des risques Informatiques Optimisés par Niveau)**

- *Repose sur des questionnaires relatifs à 6 domaines :*
  - Sécurité organisationnelle
  - Sécurité physique
  - Continuité
  - Organisation informatique
  - Sécurité logique et exploitation
  - Sécurité des applications
- *Le déroulement:*
  - Phase 0: Définition des objectifs de sécurité et du champ d'action
  - Phase 1: Audit des vulnérabilités (questionnaires) →Rosace
  - Phase 2: Analyse des risques
  - Phase3: Elaboration du plan d'action

CH3: Les attaques

- Une attaque: est une activité malveillante qui consiste à exploiter une faille d'un système informatique
- Principe général des attaques
  1. collecte d'informations
  2. repérage des lieux et détermination des vulnérabilités
  3. Réalisation de l'attaque
  4. Effacement des traces
- catégories principales d'attaque :

- **L'accès**: est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information.
  1. *Le sniffing:* Cette attaque est utilisée par les pirates informatiques pour obtenir des mots de passe.
  2. *Chevaux de Troie*: En général, le but d'un cheval de Troie est de créer une porte dérobée(backdoor) pour qu'un pirate informatique puisse ensuite accéder facilement l'ordinateur ou le réseau informatique.
  3. *L'ingénierie sociale:* n'est pas vraiment une attaque informatique, c'est plutôt une méthode pour obtenir des informations sur un système ou des mots de passe.
  4. *Le craquage des mots de passe:* consiste à faire de nombreux essais jusqu'à trouver le bon mot de passe.

  Il existe deux grandes méthodes :
  - L'utilisation de dictionnaires: le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci
  - ·La méthode brute: toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution.
- **La modification**: consiste, pour un attaquant à tenter de modifier des informations. Ce type d'attaque est dirigé contre l'intégrité de l'information.
  - Virus, ver, cheval de Troie:

    un virus est définit comme un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs.

    On classe les virus d'après leur mode de propagation et de multiplication:

        - Les vers capables de se propager dans le réseau;
        - Les « chevaux de Troie » créant des failles dans un système;
        - Les bombes logiques se lançant suite à un événement du système
        - Les canulars envoyés par mail.
    - **Le déni de service (par saturation) :** consiste à bloquer l'accès aux sites, sans en altérer le contenu. Ces attaques visent la disponibilité des informations
        0. Le flooding: consiste à envoyer à une machine de nombreux paquets IP de grosse taille.
        1. Le TCP-SYN flooding: variante du flooding qui s'appuie sur une faille du protocole TCP .
        2. Le smurf: s'appuie sur le ping et les serveurs de broadcast .
        3. Le débordement de tampon: se base sur une faille du protocole IP.
    - **La répudiation**: consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soient réellement passés. C'est une attaque contre la responsabilité.
        0. Le IP spoofing: consiste à se faire passer pour une autre machine en falsifiant son adresse IP.
        1. Le MAC spoofing: consiste à usurper l'adresse MAC d'une machine autorisée

- <u>Etude de quelques Attaques applicatives:</u>
    - **Le Cross Site Scripting (XSS):** est une attaque exploitant une faiblesse d'un site web qui valide mal ses paramètres en entrée.

      La faille XSS permet d'exécuter des scripts du coté client.
    - **CSRF (Cross Site Request Forgery):** permet à un attaquant de forcer ses victimes à effectuer certaines actions sur un site cible, sans qu'elles s'en aperçoivent.
    - **Injection SQL**: modifier une requête SQL en injectant des morceaux de code non-filtrés, généralement par le biais d'un formulaire.