Bases de la sécurité

Objectifs

- Connaître la terminologie liée à la sécurité de l'information et l'utiliser de manière adéquate
- Savoir expliquer les principes de base de la sécurité
- Savoir présenter des sources de menaces, des vulnérabilités et un scénario d'attaque
- Pouvoir évaluer les conséquences d'une attaque et sa probabilité

Notions importantes

- Sécurité de l'information:
  - Préservation
    - de la **confidentialité** (**C**onfidentiality),
    - de **l'intégrité** (**I**ntegrity)
    - et de la **disponibilité** (**A**vailability) de l'information

C: L'information n'est pas diffusée ni divulguée à des personnes ou entités non autorisées

I: L'information est exacte et complète

A: L'information est accessible et utilisable à tout moment par les personnes ou entités autorisées

Principes de base

La sécurité globale est aussi forte que le maillon le plus faible

La sécurité parfaite est impossible

La sécurité est un processus (pas un produit)

La sécurité est inversement proportionnelle à la complexité

La sécurité dépend de la participation des utilisateurs

Analyse de risque

- Calculer le **niveau de risque**:
  - Probabilité qu'une **menace** exploite une **vulnérabilité** et cause des **dommages** à un **bien**.

- Objectifs:
  - Etablir des priorités
  - Mettre en place des contre-mesures:
    - Réduire la probabilité d'une attaque
    - Réduire les conséquences d'une attaque

Sources de menace

Définir les sources de menaces

- Menace/source de menace:
  - Quelque chose capable d'effectuer une action non-désirée ou non-autorisée contre un système
- Les sources de menaces peuvent être: naturelles/physiques:
  - Naturelles/Physiques: Incendie, inondation, séisme, etc…
  - Humaines: Hackers, cybercriminels, employés mécontents, concurrents, etc…

Vulnérabilités

Identifier les vulnérabilités

- Vulnérabilité:
  - Faille dans un **bien** ou dans une mesure de sécurité qui peut être **exploitée** par une ou plusieurs **menaces**
- Exemples de vulnérabilités:
  - Mauvaise configuration
  - Utilisation de protocoles obsolètes
  - Employés mal informés
  - …

Exploitation

Evaluer la probabilité de l'exploitation d'une vulnérabilité

- Le but d'une attaque est d'exploiter une vulnérabilité pour causer des dommages à un bien
- La probabilité qu'une vulnérabilité soit exploitée dépend de:
  - La complexité de l'attaque
  - L'intérêt que représente le bien pour les sources de menace

Conséquences

Déterminer les conséquences de l'exploitation d'une vulnérabilité

- 2 types de conséquences:
  - Directes: quels aspects techniques sont impactés?
    - Perte de confidentialité de l'information
    - Perte d'intégrité de l'information
    - Perte de disponibilité de l'information
  - Indirectes: quels aspects business sont impactés?
    - Perte financière
    - Perte de réputation
    - Perte de temps de travail
    - …

Domaines de la sécurité informatique

- Les failles peuvent se trouver dans:
  - Une application web
  - Une application mobile
  - **Un réseau**
  - Un logiciel
  - Un système d'exploitation
  - Une base de données
  - Un employé
  - …
- Chacun de ces éléments correspond à un domaine de la sécurité informatique

Sécurité des réseaux

- La sécurité des réseaux concerne toutes les couches
- Enjeux de la sécurité des réseaux:
  - S'assurer que les informations transmises ne subissent pas de modifications et ne sont accessibles que à ceux à qui elles sont destinées
  - Empêcher un attaquant de se faire passer pour quelqu'un d'autre
  - Assurer la disponibilité des services
  - Ne pas divulguer d'informations sensibles sur les services disponibles