Notion de risques : Chap.2 : Les éléments de la sécurité

mercredi 11 septembre 2024 17:10

Chapitre 2 : Les éléments de la sécurité

Objectifs

- Comprendre les différents éléments constitutifs de la sécurité informatique.
- Identifier les composants matériels et logiciels nécessaires à la protection des systèmes d'information.
- Appréhender les processus organisationnels qui renforcent la sécurité.

A. Introduction

L'introduction présente les éléments essentiels qui constituent la sécurité des systèmes d'information. Cela inclut une vue d'ensemble des aspects matériels, logiciels et humains qui interagissent pour créer une infrastructure de sécurité robuste. Nous examinerons également l'importance des politiques de sécurité dans la mise en œuvre d'une stratégie de sécurité efficace.

- **Notion d'éléments de sécurité :**
  - Les éléments de sécurité englobent les dispositifs matériels (pare-feu, systèmes de détection d'intrusion), les logiciels de sécurité (antivirus, systèmes de gestion des informations et des événements de sécurité - SIEM) et les pratiques organisationnelles (politiques de sécurité, sensibilisation des utilisateurs).

B. Concepts

B.1 : Composants Matériels :

- **Pare-feu :**
  - Dispositif de sécurité qui surveille et contrôle le trafic réseau entrant et sortant basé sur des règles de sécurité prédéfinies. Ils peuvent être matériels ou logiciels.
- **Systèmes de Détection et de Prévention des Intrusions (IDS/IPS) :**
  - Outils qui surveillent le réseau pour détecter des activités malveillantes ou des violations de politique. Un IDS peut alerter l'administrateur, tandis qu'un IPS peut agir pour bloquer les menaces.
- **Dispositifs de Sauvegarde :**
  - Solutions matérielles et logicielles qui garantissent la sauvegarde régulière des données pour prévenir la perte de données due à des défaillances matérielles ou des cyberattaques.

B.2 : Composants Logiciels :

- **Antivirus et Antimalware :**
  - Logiciels conçus pour détecter, prévenir et supprimer les malwares. Ils jouent un rôle essentiel dans la protection des systèmes contre les virus, vers et ransomwares.
- **Systèmes de Gestion des Informations et des Événements de Sécurité (SIEM) :**
  - Solutions qui collectent et analysent les données de sécurité en temps réel pour fournir

une vue d'ensemble des incidents et permettre une réponse rapide.

B.3 : Processus Organisationnels :

- **Politiques de Sécurité :**
  - Documentations formelles qui définissent les règles et les procédures pour protéger les informations sensibles. Elles guident les employés sur les comportements à adopter pour maintenir la sécurité.
- **Sensibilisation et Formation :**
  - Programmes destinés à éduquer les employés sur les pratiques de sécurité, les risques potentiels et les procédures à suivre en cas d'incident.

C. Référentiel…

- **Normes et Cadres de Référence :**
  - **ISO/IEC 27001 :**
    - Norme internationale qui définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un système de gestion de la sécurité de l'information.
  - **NIST Cybersecurity Framework :**
    - Cadre qui offre une approche flexible pour la gestion des risques en cybersécurité, en intégrant des éléments techniques et organisationnels.
  - **CIS Controls :**
    - Ensemble de meilleures pratiques pour améliorer la sécurité des systèmes d'information. Ils sont souvent utilisés comme base pour la mise en œuvre des contrôles de sécurité.