Notion de risques : Chap.9 : Analyse des risques

mercredi 11 septembre 2024 17:10

Chapitre 9 : Analyse des risques

Objectifs

- Comprendre l'importance de l'analyse des risques dans la gestion de la sécurité des systèmes d'information.
- Identifier les différentes étapes et méthodologies pour réaliser une analyse des risques efficace.
- Appréhender les meilleures pratiques pour la gestion des risques identifiés.

A. **Introduction**

L'analyse des risques est une composante essentielle de la gestion de la sécurité des systèmes d'information. Elle permet d'identifier, d'évaluer et de prioriser les risques potentiels qui pourraient compromettre la sécurité des informations. Une analyse rigoureuse aide les organisations à mettre en œuvre des mesures de sécurité appropriées pour protéger leurs actifs critiques. Ce chapitre se concentre sur les concepts fondamentaux de l'analyse des risques, les méthodologies utilisées et les meilleures pratiques à suivre.

B. Concepts

B.1 : Importance de l'Analyse des Risques :

- L'analyse des risques permet de comprendre les menaces potentielles et d'évaluer leur impact sur l'organisation. Cela aide à allouer efficacement les ressources pour la sécurité et à établir des priorités dans les actions à entreprendre.

B.2 : Étapes de l'Analyse des Risques :

- **Identification des Risques :**
  - Identifier les actifs, les menaces et les vulnérabilités potentielles. Cela inclut des sources de menaces internes et externes, telles que les cyberattaques, les erreurs humaines et les catastrophes naturelles.
- **Évaluation des Risques :**
  - Évaluer la probabilité de survenue de chaque risque et l'impact potentiel sur l'organisation. Cela peut être fait à l'aide de méthodes qualitatives ou quantitatives.
- **Priorisation des Risques :**
  - Classer les risques en fonction de leur **niveau de gravité** et de leur **probabilité d'occurrence**, afin de déterminer les mesures à prendre en priorité.

B.3 : Méthodologies d'Analyse des Risques

- **Méthode Qualitative :**
  - Utilise des descriptions et des classements pour évaluer les risques, permettant une compréhension intuitive des menaces sans nécessiter des données chiffrées précises.
- **Méthode Quantitative :**
  - Implique l'utilisation de données chiffrées pour évaluer les risques, fournissant une

approche plus objective et mesurable. Cela peut inclure des modèles mathématiques et des analyses de scénarios.

- **Approche basée sur les scénarios :**
  - Évaluation des impacts potentiels en simulant des scénarios d'incidents pour comprendre comment différentes menaces pourraient affecter l'organisation.

C. Référentiel…

- **Normes et Cadres de Référence :**
  - **ISO/IEC 27005 :** Norme internationale. Sécurité de l'information, cybersécurité et protection de la vie privée - Préconisations pour la gestion des risques liés à la sécurité de l'information
  - **ISO 31000 :**
    - Norme internationale pour la gestion des risques, offrant des lignes directrices pour l'intégration de la gestion des risques dans les processus organisationnels.
  - **NIST SP 800-30 :**
    - Publication qui fournit des recommandations pour l'analyse des risques dans les systèmes d'information.
- **Meilleures Pratiques :**
  - **Documentation :**
    - Documenter chaque étape de l'analyse des risques, y compris les méthodes utilisées, les résultats obtenus et les décisions prises.
  - **Réévaluation Régulière :**
    - Effectuer des analyses des risques régulièrement pour tenir compte des évolutions technologiques, des nouvelles menaces et des changements dans l'organisation.

D. Meilleurs pratiques inspirés des référentiels de normalisation…

- Pour faire une analyse des risques, s'appuyer sur des audits internes/externes peut-être un bon début avant de se lancer à introduire une norme tel que la norme ISO27001. Mais aussi s'appuyer sur des bonnes pratiques (ITIL) en ne sélectionnant que les thèmes techniques (14) permet aussi d'évaluer les efforts qu'il faut consentir pour transformer son SMSI en système normé.