Notion de risques : Chap.1 : Notions de sécurité, de risque, de qualité.

mercredi 11 septembre 2024 17:10

Chapitre 1 : Notions de sécurité, de risque, de qualité.

Objectifs

- Apprendre les notions de sécurité, de risque et de qualité en informatique.
- Comprendre les concepts fondamentaux de la sécurité informatique.
- Identifier et définir les risques associés aux systèmes d'information.
- Présenter les normes de qualité en matière de sécurité et leur importance dans la gestion des systèmes d'information.

A. Introduction

Introduction aux concepts fondamentaux de la sécurité informatique, définition des risques associés aux systèmes d'information et présentation des normes de qualité en matière de sécurité.

Définition selon IBM :

- Qu'est-ce que la sécurité informatique ? | IBM
- Chap.1 : IBM

- **Notion de sécurité en informatique :**
  - La sécurité en informatique couvre divers domaines, éléments et méthodes. Elle inclut tout aussi bien des éléments physiques, des postes clients jusqu'aux éléments du réseau et des systèmes, mais aussi les biens immatériels (logiciels - données). Elle prend en compte l'interaction humaine, notamment les processus de l'entreprise et la protection des personnes. Elle vise donc la protection des données, des systèmes matériels et des réseaux contre les accès non autorisés, les attaques, les pertes ou les destructions, mais aussi des êtres humains.
- **Définition de la sécurité informatique :**
  - La sécurité informatique désigne l'ensemble des mesures et pratiques visant à protéger les systèmes d'information contre les accès non autorisés, les perturbations, les destructions et les modifications malveillantes.
- **Notion de risques en informatique :**
  - Les risques en informatique se réfèrent à la **probabilité** qu'une menace exploitant une vulnérabilité entraîne des conséquences négatives pour les actifs d'information. Les risques peuvent provenir de divers facteurs, y compris des erreurs humaines, des défaillances techniques, des catastrophes naturelles et des actes malveillants.
- **Définition de risques en informatique :**
  - Un risque informatique est généralement défini comme une combinaison de la probabilité qu'un événement indésirable se produise (par exemple, une violation de données ou une panne système) et de l'impact potentiel de cet événement sur l'organisation. Cela implique une évaluation continue des menaces et des vulnérabilités associées aux systèmes d'information.
- **Notion de qualité en informatique :**
  - La qualité en informatique désigne le degré auquel un système, un produit ou un service répond aux exigences et attentes spécifiées. Dans le contexte de la sécurité informatique, la qualité englobe la fiabilité, la disponibilité, la performance et la conformité aux normes de

sécurité établies.

- **Définition de qualité en informatique :**
  - La qualité en matière de sécurité informatique se réfère aux caractéristiques qui assurent que les systèmes d'information sont protégés de manière adéquate contre les menaces, tout en répondant aux besoins de l'utilisateur et aux exigences réglementaires. Cela comprend la mise en œuvre de politiques de sécurité, l'évaluation des performances des systèmes et l'amélioration continue des processus de sécurité.

B. Concepts

Sécurité informatique :

Les trois piliers de la cybersécurité :

- **Confidentialité :** Protection des informations contre les accès non autorisés.
  - La confidentialité vise à garantir que seules les personnes autorisées ont accès à des informations sensibles. Cela implique des mesures telles que le chiffrement des données, les contrôles d'accès et la gestion des identités.
- **Intégrité :** Assurance que les informations ne sont pas altérées ou supprimées de manière non autorisée.
  - L'intégrité concerne la protection des données contre les modifications non autorisées. Cela inclut l'utilisation de mécanismes comme les signatures numériques et les sommes de contrôle pour s'assurer que les données n'ont pas été altérées durant leur stockage ou leur transmission.
- **Disponibilité :** Garantir que les utilisateurs autorisés peuvent accéder aux informations et systèmes nécessaires.
  - La disponibilité assure que les systèmes et les données sont accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin. Cela nécessite la mise en place de solutions de sauvegarde, de redondance et de récupération après sinistre.

Risques Associés aux Systèmes d'Information

- **Concept de risque :**
  Un risque en matière de sécurité informatique est défini comme la probabilité qu'un événement indésirable se produise, combinée à l'impact potentiel de cet événement sur les systèmes d'information.
- **Types de risques :**
  - **Risques techniques :** Pannes de matériel, vulnérabilités logicielles, attaques par malware.
    - Incluent les pannes matérielles, les bugs logiciels, les attaques par malware et les défaillances de réseau. L'analyse de ces risques nécessite une compréhension des vulnérabilités techniques et de l'environnement informatique.
  - **Risques humains :** Erreurs de manipulation, ingénierie sociale, négligence.
    - Proviennent des erreurs humaines, de la négligence ou de comportements malveillants, tels que le phishing. La sensibilisation et la formation des utilisateurs sont essentielles pour atténuer ces risques.
  - **Risques environnementaux :** Catastrophes naturelles, pannes d'électricité, incendies.
    - Concernent les catastrophes naturelles (inondations, incendies) et les incidents liés à l'infrastructure physique. L'analyse de ces risques implique des évaluations d'impact et des plans d'urgence.
- **Analyse des risques :**
  - **Identifier les menaces**, évaluer les vulnérabilités et déterminer leurs impacts.
  - L'analyse des risques implique l'identification, l'évaluation et la priorisation des menaces potentielles, suivies par la mise en œuvre de mesures de mitigation(atténuation). Cette approche permet de renforcer la posture de sécurité d'une organisation.

Qualité en Informatique

La qualité en informatique se décline en plusieurs dimensions :

- **Qualité des Produits :**
  - Cela inclut les logiciels et systèmes, qui doivent répondre à des critères tels que la fonctionnalité, la fiabilité, et la performance. Les normes telles que **ISO 9001** peuvent servir de cadre pour évaluer la qualité.
- **Qualité des Processus :**
  - Les méthodes de développement et de gestion de projet (par exemple, Agile, DevOps) doivent être adaptées pour garantir une qualité élevée tout au long du cycle de vie du produit.
- **Qualité des Services :**
  - La qualité des services informatiques se réfère à la capacité à fournir un support et une maintenance efficaces, garantissant que les systèmes fonctionnent comme prévu et répondent aux attentes des utilisateurs.
  - Un cadre reconnu pour la gestion de la qualité des services est ITIL, qui fournit des bonnes pratiques pour la gestion des services informatiques. ITIL se concentre sur l'alignement des services informatiques avec les besoins de l'entreprise et comprend des processus tels que la gestion des incidents, la gestion des problèmes et la gestion des changements. En appliquant les principes d'ITIL, les organisations peuvent améliorer la satisfaction des utilisateurs et optimiser l'efficacité des services fournis.

C. Référentiel des Normes de Qualité en Matière de Sécurité

- **Importance des normes de qualité :**
  Les normes de qualité fournissent un cadre pour garantir la sécurité des systèmes d'information, aider à la conformité réglementaire et établir des meilleures pratiques.
- **Normes courantes :**
  - **ISO/IEC 27001 :** Norme internationale. Sécurité de l'information, cybersécurité et protection de la vie privée - Système de management de la Sécurité de l'Information (SMSI).
  - **ISO/IEC 27002 :** Norme internationale. Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité de l'Information.
  - **NIST Cybersecurity Framework :** Cadre développé par le National Institute of Standards and Technology pour améliorer la gestion des risques de cybersécurité.
  - **PCI DSS (Payment Card Industry Data Security Standard) :** Norme de sécurité pour les entreprises qui traitent des paiements par carte de crédit.
  - **ISO 9001-2015** : Systèmes de management de la qualité