Chapitre 4 - Gouvernance de sécurité

Yann-Arzel

27 juillet 2023

- Organisation des entreprises
- Gouvernance : cadre, méthodologie, objectifs
- Comment raisonne un Responsable de la sécurité de l'information (RSSI) ?

Construction de la Politique de sécurité du système d'information

Soustitre

Contenu du texte ce que l'on veut comme par exemple

- Définition d'une politique de sécurité
- Intégration de la politique de sécurité dans la gouvernance du SI

La politique de sécurité générale (PSG) est généralement basée sur l'architecture de l'ISO/EIC 27001, et donne le cadre général de conformité pour les projets, les organisations sous-jacentes (divisions, filiales), les produits ainsi que l'organisation des responsabilités.
Cette PSG est déclinée en différentes politiques de sécurité par secteurs (souvent structurées par les chapitres de l'ISO/EIC 27001)

- IAM
- Filtrage et sécurité périmétrique
- Détection et rémédiation
- continuité d'activité

- Identification des biens essentiels à protéger
- Intégration dans la politique de sécurité

- Gestion de l'administration des équipements
  - protocoles d'accès autorisés : SSHv3, HTTPs, interdiction de TELNET
  - protocoles de supervision autorisés : SNMPv3
- Politique de mot de passe
- Gestion des fournisseurs

1. Présentation de la norme ISO/EIC 27001
2. Périmètre de certification
3. Mesures de sécurité : ISO/EIC 27002

Quel est le but d'ISO 27k1 ? Pourquoi l'utiliser ?

Périmètre de certification

- Quel est le périmètre de certification ?
- SOA : définition, rôle

- Définition mesures de sécurité
- Exemples

Audit de conformité

DASHBOARD niveau de sécurité

Exemples :

- nb d'incidents critiques
- % remediation vulnérabilité critiques
- %parc administrés suivant les règles de la politique
- nombre de PKI déployées, %PKI dans les équipes sécurité incluses dans le périmètre de certification
- % de personnes sensibilisées

- Business Impact Analysis (BIA)
- Business Continuity Plan (BCP)
- Plan de Continuité d'Activité (PCA) / Disaster Recovery Plan (DRP)
- Plan de Reprise d'Activité (PRA)