4 - Management de la sécurité

Eléments de cybersécurité d'entreprise

Yann-Arzel LE VILLIO

yannarzel.levillio@orange.com

http://campus.orange.com

CyberSkills4All
Direction technique & scientifique OSS

Publication Eléments de cours CYBERSKILLS4ALL

CYBERDEF 101
Eléments de cybersécurité et de cyberdéfense d'entreprise

orange™

Abstract

Hashtags : Gouvernance, SMSI, ISO27001, ISO27002, ISO22301, BCCM BCP, PRA, PCA

Ce document présente comment **appréhender les enjeux de conformité et de pilotage du client** afin d'être à même de lister les biens à protéger dans une politique de sécurité et de définir un système de management de sécurité conformes aux normes ISO.Comprendre le périmètre de certification et les plans de continuité définis afin de valider les mesures de sécurité et d'organiser les audits de conformité

Sommaire

Gouvernance et management de la sécurité

- # 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

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

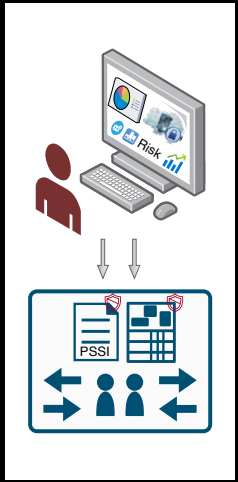
Concept de PSG

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

Yann-Arzel LE VILLIO

AR2PSSI



Approche par les risques

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

Exemples de chapitres de PSSI

- 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

Système de management de la sécurité de l'information : SMSI

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

Very short intro to ISO/EIC 27001

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

Périmètre de certification

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

ISO/EIC27002

- # Définition mesures de sécurité
- # Exemples

Audit de conformité

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

Continuité d'activité : ISO22301

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

Conclusion Management de la sécurité

- La sécurité de l'information est un enjeu stratégique pour toute organisation, indispensable pour protéger ses actifs, assurer la confiance et respecter les obligations réglementaires
- La Politique de Sécurité des Systèmes d'Information (PSSI) constitue le socle de la démarche : elle s'appuie sur une analyse de risques, définit les objectifs, les règles et les responsabilités, et doit être comprise et appliquée par tous
- Le Système de Management de la Sécurité de l'Information (SMSI), basé sur la norme ISO 27001, structure la gestion de la sécurité autour de processus clairs, d'une amélioration continue (cycle PDCA) et d'un engagement fort de la direction
- Les audits organisationnels et les tableaux de bord permettent de piloter la sécurité, de démontrer la conformité et d'identifier les axes d'amélioration
- La continuité d'activité (ISO 22301) complète la démarche en préparant l'organisation à faire face aux incidents majeurs et à maintenir ses fonctions critiques

Conclusion Management de la sécurité

- o

des questions ?

Contributions

Les notes et les présentations sont réalisées sous LaTeX.
Vous pouvez contribuer au projet du cours CYBERDEF101. Les contributions peuvent se faire sous deux formes :

- Corriger, amender, améliorer les notes publiées. A chaque session des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de vos expertises dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBERDEF101) [a].

a. https://github.com/edufaction/CYBERDEF101

Mises à jour régulières

Vérifiez la disponibilité d'une version plus récente de

L-Orange-Cyberdef101-M4c-Management.przt.pdf sur GITHUB CYBERDEF [1]