Orange CyberSchool, Direction de la formation
Notes de cours éditées le 6 décembre 2024, 21 h 10 CET

Sécurité dans les projets

Yann-Arzel LE VILLIO[1,2]*

Résumé
Ce document présente comment différentier la sécurité dans les projets et la sécurité de l'entreprise afin de découvrir les règles techniques de sécurisation des composants du SI, l'organisation des équipes sécurité dans les projets et les enjeux de conformité technique des produits
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information, de la cybersécurité, et de la cyberdéfense. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document unique, mais édité par chapitre dans le cadre de ce cours.
Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cyberdéfense d'entreprise.

Mots clefs
Hardening, ITIL, ANSSI, CSPN

[1] *Enseignant Sécurité ESIR*
[2] *Directeur Technique et Scientifique Orange CyberSchool*
***email** : yann-arzel.levillio@orange.com –

Eléments de cours

Vérifiez la disponibilité d'une version plus récente de

L-Orange-Cyberdef101-M6c-Secuprojet.doc.pdf sur GITHUB CYBERDEF [1]

1. https://github.com/edufaction/CYBERDEF/raw/master/Builder/L-Orange-Cyberdef101-M6c-Secuprojet.doc.pdf

Table des matières

1. Introduction Product

PROCESS type SECU In TTM : Secu by design, secu les projets vs securité d'entreprise (Ingénierie de la sécurité, OPERATION et PROJET) - Sécurité des produits (ISO 15504, CSPN …)

différentier la sécurité dans les projets et la sécurité de l'entreprise afin de découvrir les règles techniques de sécurisation des composants du SI, l'organisation des équipes sécurité dans les projets et les enjeux de conformité technique des produits

2. Règles techniques de sécurisation : durcissement

Les actions de durcissement, en anglais hardening, consistent à améliorer le niveau de sécurité des systèmes via des actions de configuration, choix techniques et process.

Le durcissement s'inscrit naturellement dans le process de conception securisée par défaut, security by design en anglais. Il est tout aussi important que le maintien en condition opérationnelle et sécurisé et peut réduire significativement les risques cyber.

2.1 IAM

(PKI, MFA, journalisation, contrôles)

Pourquoi déployer une infrastructure de gestion de clés ? Voir au chapitre 3 les principes cryptographiques et fonctionnalités des IGC (PKI).

2.2 Systèmes d'exploitation

Hardening UNIX/WINDOWS kesako ? ACL, admin dédié, supervision et administration via réseau chiffré, tout doit être loggé ! Exclusion services inutiles 80 443 principe qui se décline sur toutes les applis

2.3 Hardware (HSM), DC

Chiffrement, zone hardware dédiée (mémoire, voire carte dédiée), DC : salles, controles d'accès, caméras, vigiles, etc.

2.4 Réseaux

VPN, chiffrement

- #CIS, #ACL
- #hardening, #HSM,

3. Organisation de la sécurité dans les projets

ingénierie, opération, pilotage Schéma relations entre les différentes équipes

- Ingénierie : missions
- Opération : missions
- Pilotage : missions

4. Sécurité des produits

La conformité technique aux référentiels/normes est un élément fondamental pour s'assurer que les produits logiciels et hardware sont conformes aux normes et réglementations du secteur.

4.1 Conformité aux implémentations normatives

- Protocoles réseaux
- Normes environnementales

4.2 La confiance certifiée

Dans le domaine de la cybersécurité on peut faire certifier des produits logiciels ou matériels avec la Certification de Sécurité de Premier Niveau (CSPN) ou les critères communs. En France cela passe par l'ANSSI.

4.2.1 Certification de Sécurité de Premier Niveau (CSPN)

La CSPN mise en place par l'ANSSI en 2008 consiste en des tests en « boîte noire » effectués en temps et délais contraints. La CSPN est une alternative aux évaluations Critères Communs, dont le coût et la durée peuvent être un obstacle, et lorsque le niveau de confiance visé est moins élevé. Cette certification s'appuie sur des critères, une méthodologie et un processus élaborés par l'ANSSI publiés sur le présent site. (source ANSSI)

4.2.2 critères communs

La certification dite tierce partie est la certification de plus haut niveau, qui permet à un client de s'assurer par l'intervention d'un professionnel indépendant, compétent et contrôlé, appelé organisme certificateur, de la conformité d'un produit à un cahier des charges ou à une spécification technique.

La certification tierce partie apporte au client la confirmation indépendante et impartiale qu'un produit répond à un cahier des charges ou à des spécifications techniques publiées. Ces spécifications techniques peuvent être élaborées dans un cadre normatif ou non. (source ANSSI) AJOUTER EXEMPLES

-
-

5. Security By Design : concepts et méthodologies

5.1 Définition et principes fondamentaux

5.2 Intégration de la sécurité dans le cycle de développement logiciel

5.3 Méthodologies de conception sécurisée

5.3.1 Threat modeling

5.3.2 Analyse de risques

5.3.3 Privacy by design

6. Règles techniques de sécurisation et durcissement

6.1 Sécurisation des systèmes d'exploitation

6.1.1 Mise à jour et gestion des correctifs

6.1.2 Configuration des paramètres de sécurité

9.1 Certification de Sécurité de Premier Niveau (CSPN)

9.1.1 Objectifs et processus

9.1.2 Critères d'évaluation

9.2 Critères Communs

9.2.1 Niveaux d'assurance

9.2.2 Processus de certification

9.3 Importance de la conformité dans le cycle de développement

10. Mise en pratique et études de cas

10.1 Analyse d'incidents de sécurité réels

10.2 Exercices de sécurisation d'une infrastructure

10.3 Évaluation et amélioration continue des mesures de sécurité