CyberSkills4All, par Orange Security School
Notes de cours éditées le 18 décembre 2024, 16 h 11 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 Security School*
***email** : yannarzel.levillio@orange.com –

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

Table des matières

1. Introduction Product

Ce chapitre se propose d'explorer la distinction entre la sécurité dans les projets et la sécurité de l'entreprise, deux concepts souvent confondus mais aux implications différentes.

Nous aborderons les règles techniques essentielles pour sécuriser les composants des systèmes d'information (SI), ainsi que l'organisation des équipes de sécurité au sein des projets. Enfin, nous mettrons en lumière les enjeux de conformité technique des produits, afin de garantir une approche intégrée et efficace de la sécurité dans le développement de projets. Cette compréhension approfondie est cruciale pour anticiper les risques et assurer la pérennité des initiatives numériques.

2. Security By Design

Le concept de **Security By Design** s'impose comme une approche fondamentale dans le développement de systèmes et d'applications sécurisés. Nous aborderons dans ce chapitre les principes clés de cette "philosophie", qui intègre la sécurité dès les premières étapes de conception, plutôt que de l'ajouter en fin de processus. Nous examinerons les éléments essentiels qui sous-tendent cette démarche proactive, tels que **l'évaluation des risques**, **la minimisation des surfaces d'attaque** et l'implémentation de **contrôles de sécurité robustes**.

Dans un second temps, nous aborderons les méthodes de **maintien en condition de sécurité (MCS)**, qui garantissent que les systèmes restent protégés tout au long de leur cycle de vie. Cela inclut des pratiques telles que la **surveillance continue**, **les mises à jour régulières** et **les audits de sécurité**, permettant ainsi d'adapter les mesures de protection face à l'évolution des menaces.

En intégrant ces deux volets, ce chapitre vise à fournir une compréhension complète du Security By Design et de son rôle crucial dans la sécurité des projets.

2.1 Concepts et principes

Ce chapitre se penchera d'abord sur les principes clés du security by design. Parmi ceux-ci, l'évaluation des risques joue un rôle central. Cette activité implique d'identifier les vulnérabilités potentielles et d'analyser les impacts possibles sur les systèmes et les données. Une évaluation rigoureuse permet de prioriser les efforts de sécurité en fonction des menaces les plus critiques (cf. chapitre 4.1 pour plus de détails sur les diffréntes méthodes d'analyse de risques).

Ensuite, la minimisation des surfaces d'attaque qui consiste à réduire le nombre de points d'entrée potentiels pour les attaquants, en limitant les fonctionnalités non essentielles et en appliquant le principe du moindre privilège. En restreignant l'accès aux ressources et en désactivant les services inutilisés, les organisations peuvent considérablement diminuer leur exposition aux cyberattaques. Nous reverrons ce sujet dans le chapitre suivant sur le durcissement.

Enfin, l'implémentation de contrôles de sécurité robustes est essentielle pour garantir la protection des systèmes. Cela inclut l'intégration de mécanismes de sécurité tels que l'authentification forte, le chiffrement des données et la surveillance des activités suspectes. Ces contrôles doivent être conçus pour fonctionner de manière cohérente tout au long du cycle de vie du produit, assurant ainsi une défense en profondeur.

2.2 Méthodes de MCS (Maintien en Condition de Sécurité)

On appelle méthodes de maintien en condition de sécurité ou **MCS** les méthodes qui garantissent que les systèmes restent protégés tout au long de leur cycle de vie. Ces pratiques sont essentielles pour s'assurer que les mesures de sécurité initialement mises en place continuent d'être efficaces face à l'évolution constante des menaces ou l'apparition de vulnérabilités. Nous verrons par la suite les méthodes de surveillance continue, d'application des mises à jour régulières, l'utilisation des audits de sécurité et enfin la sensibilisation des utilisateurs.

2.2.1 Surveillance Continue

La surveillance continue est une méthode et une activité clé pour détecter et répondre rapidement aux incidents de sécurité. Cela implique l'utilisation par exemple de systèmes de détection d'intrusion (IDS) (cf. chapitre 3.3) et de solutions de gestion des informations et de corrélation des événements de sécurité (SIEM). Par exemple, une entreprise peut déployer un SIEM pour collecter, analyser et corréler les journaux d'activité de ses serveurs et applications. En surveillant ces données en temps réel, l'organisation peut identifier des comportements anormaux, tels que des tentatives de connexion suspectes ou d'exfiltration de données, et réagir rapidement pour atténuer les risques et dommages en isolant des serveurs ou en coupant des flux au niveau des pare feux par exemple.

2.2.2 Mises à Jour Régulières

Les mises à jour régulières des logiciels et des systèmes sont cruciales pour maintenir leur sécurité. Les vulnérabilités découvertes dans les logiciels doivent être corrigées par des mises à jour fournies par les éditeurs. Par exemple, un système d'exploitation peut recevoir des correctifs mensuels pour combler des failles de sécurité. Ignorer ces mises à jour expose les systèmes à des attaques exploitant ces vulnérabilités. Ainsi, établir un processus de gestion des correctifs, qui inclut l'évaluation et l'application rapide et régulière des mises à jour, est essentiel pour protéger les environnements numériques.

2.2.3 Audits de Sécurité

Les audits de sécurité, tels que les tests d'intrusion et les évaluations de vulnérabilité, sont également des pratiques importantes pour maintenir la sécurité. Par exemple, une entreprise peut engager des experts en sécurité pour réaliser des tests d'intrusion sur son système d'information. Ces tests simulent des attaques réelles afin d'identifier les failles de sécurité avant qu'elles ne soient exploitées par des attaquants. De plus, des évaluations régulières des vulnérabilités permettent de détecter les points faibles et d'appliquer des mesures correctives. Les rapports de ces tests permettent aux propriétaires et acteurs du système de consolider et maintenir la sécurité de leur produit. Ces tests peuvent être faits au plus tôt dans la phase de conception mais aussi (et surtout !) tout au long de la vie du système.

2.2.4 Formation et Sensibilisation

Enfin, la formation et la sensibilisation des employés jouent un rôle crucial dans le maintien de la sécurité. Les utilisateurs finaux sont souvent la première ligne de défense contre les cybermenaces. Par exemple, des sessions de formation régulières sur la reconnaissance des tentatives de phishing et les bonnes pratiques de sécurité peuvent réduire considérablement le risque d'incidents liés à l'erreur humaine.

3. 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 décrit dans le chapitre précédent. Il est tout aussi important que le maintien en condition opérationnelle et sécurisé et peut réduire significativement les risques cyber.

3.1 IAM

(PKI, MFA, journalisation, contrôles)

Pourquoi déployer une infrastructure de gestion de clés ?

La mise en place d'une infrastructure de gestion de clés (PKI) est essentielle pour garantir la sécurité des communications et des transactions numériques. En intégrant des mécanismes tels que l'authentification à facteurs multiples (MFA), les organisations renforcent la protection des accès en exigeant plusieurs preuves d'identité. Cette méthode utilise le principe de coupler un élément que l'on possède (carte ou donc ici une clé PKI par exemple) et que l'on connait (mot de passe, ou réponse à une question).

De plus, la journalisation des activités permet de suivre et d'analyser les accès et les modifications, assurant ainsi un suivi et une traçabilité indispensable en cas d'incident.

Enfin, l'implémentation de contrôles permet de gérer efficacement les clés cryptographiques, de la création jusqu'à la destruction, réduisant ainsi les risques de compromission et assurant la confidentialité et l'intégrité des données.

Voir au chapitre 3 les principes cryptographiques et fonctionnalités des IGC (PKI).

3.2 Systèmes d'exploitation et applications

Les systèmes d'exploitation Windows, Linux et même MacOS sont des cibles privilégiées par les attaquants. Il est donc important qu'ils soient configurés afin d'être le moins possible vulnérable à des attaques. Le Center for Internet Security (CIS) propose des configurations types pour chaque système et il est recommandé de les appliquer. Ces recommandations et configurations sont appelés "durcissement des systèmes d'exploitation" car le but est bien de renforcer la sécurité.

Par exemple, pour les environnements UNIX/Linux, l'activation de SeLinux est recommandée, tandis que pour Windows, l'utilisation de stratégies de groupe (GPO) et d'AppLocker est conseillée. En ce qui concerne les applications, il est important de ne pas afficher publiquement la version utilisée et d'appliquer des règles de conception visant à protéger les données confidentielles.

L'administration des réseaux et des systèmes doit également suivre des pratiques de mises en oeuvre sécurisées, telles que l'utilisation de listes de contrôle d'accès (ACL) afin de limiter les accès aux réseaux et utilisateurs spécifiques. Il est conseillé de séparer le réseau d'administration des autres réseaux de l'entreprise et de réaliser la supervision via un réseau chiffré, en utilisant des protocoles sécurisés comme SNMPv3 et SSH. De plus, il est essentiel de remplacer les mots de passe par défaut par des mots de passe forts et de les stocker dans une base de données sécurisée (coffre fort numérique).

Sur tous les systèmes, OS, application ou même réseaux, il convient d'exclure les services inutiles, en faisant attention aux serveurs web qui peuvent être activés par défaut. La conservation des journaux d'événements est primordiale pour permettre une investigation efficace en cas de problème. Enfin, il est recommandé de privilégier les protocoles sécurisés, tels que HTTPS, SMTPS et IMAPS, et d'utiliser des certificats valides pour garantir la sécurité des communications.

3.3 Hardware (HSM), DC

3.4 Réseaux

VPN, chiffrement

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

4. Organisation de la sécurité dans les projets

ingénierie, opération, pilotage Schéma relations entre les différentes équipes

- Ingénierie : missions
- Opération : missions

- Pilotage : missions
-
-

5. 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.

5.1 Conformité aux implémentations normatives

- Protocoles réseaux
- Normes environnementales

5.2 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.

5.2.1 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)

5.2.2 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

-
-

6. Security By Design : concepts et méthodologies

6.1 Définition et principes fondamentaux

6.2 Intégration de la sécurité dans le cycle de développement logiciel

6.3 Méthodologies de conception sécurisée

6.3.1 Threat modeling

6.3.2 Analyse de risques

6.3.3 Privacy by design

9.2 Techniques de protection

9.2.1 Chiffrement

9.2.2 Contrôle d'accès

9.2.3 Gestion des clés

9.3 Gestion des transferts de données sécurisés

9.4 Conformité réglementaire (ex : RGPD)

10. Conformité des produits

10.1 Certification de Sécurité de Premier Niveau (CSPN)

10.1.1 Objectifs et processus

10.1.2 Critères d'évaluation

10.2 Critères Communs

10.2.1 Niveaux d'assurance

10.2.2 Processus de certification

10.3 Importance de la conformité dans le cycle de développement

11. Mise en pratique et études de cas

11.1 Analyse d'incidents de sécurité réels

11.2 Exercices de sécurisation d'une infrastructure

11.3 Évaluation et amélioration continue des mesures de sécurité