CyberSkills4All, par Orange Security School
Notes de cours éditées le 28 février 2025, 15 h 54 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 –

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

Table des figures

1. Introduction

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 (et donc trop tard !). 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 différentes méthodes d'analyse de risques).

Ensuite, la minimisation des surfaces d'attaque 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. l'exemple ci-dessous représente schématiquement un système ou seul les ports liés au fonctionnement du serveur de base de données sont ouverts. Nous reverrons ce sujet et son application technique 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

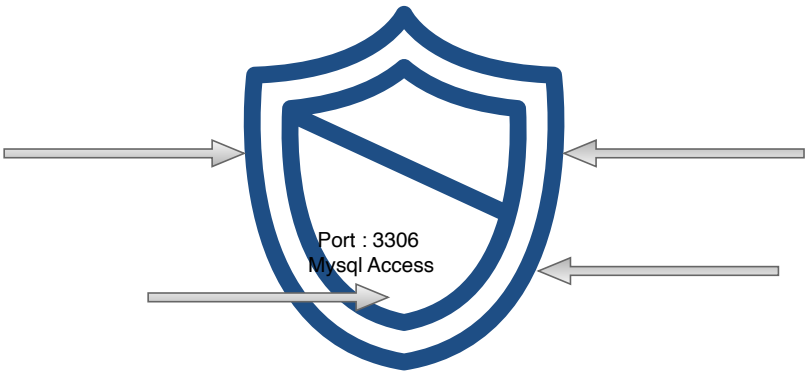

Figure 1. Minimisation : exemple d'un serveur de Base de données

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 sécurisée et peut réduire significativement les risques cyber (ce qui est bien évidemment le but final).

Ce chapitre décrit les différentes techniques de sécurisation appliquées à la gestion des droits et accès, les systèmes d'exploitation et applications, le matériel (bâtiments, équipements) et enfin les réseaux. La liste des exemples présentées n'est pas exhaustives et bien évidemment évolutive en fonction des avancées technologiques et des besoins de sécurisation qui peuvent évoluer dans le temps.

3.1 Sécurisation des droits et accès

Pourquoi déployer une infrastructure de gestion de clés ?

La mise en place d'une infrastructure de gestion de clés (IGC), ou Public Key Infrastructure (PKI) en anglais, 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). L'ANSSI définit dans son cyberdico la PKI [2] comme un "Ensemble organisé de composantes fournissant des services de gestion des clés cryptographiques et des certificats de clés publiques au profit d'une communauté d'utilisateurs".

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 vulnérables 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.

La liste des paramètres à appliquer peut être très longue et est mis à jour régulièrement pour adapter les configurations en fonction des nouvelles menaces. Cette liste n'est pas très éloignée des bonnes pratiques et le guide d'hygiène informatique [3] de l'ANSSI donne une base de référence pour configurer les systèmes.

Pour les environnements UNIX/Linux, voir ci-dessous quelques règles à appliquer :

- Mise à jour régulière : maintenir le système (noyau et applications !) à jour avec les derniers correctifs de sécurité.

2. PKI : https://cyber.gouv.fr/le-cyberdico#P
3. Guide d'hygiène ANSSI : https://cyber.gouv.fr/publications/guide-dhygiene-informatique

- Désactiver les services inutiles : identifier et désactiver les services et démons non nécessaires pour réduire la surface d'attaque.
- Configurer un pare-feu : utiliser iptables ou netfilter ou autres pour contrôler le trafic réseau entrant et sortant. Ce composant est, comme tous les autres, bien évidemment à configurer minutieusement car mal paramétré il ne sert à rien. Voir le chapitre 3 pour plus d'éléments sur les pare-feux.
- Utiliser SELinux (Security Enhanced Linux) ou AppArmor : activer et configurer SELinux ou AppArmor pour appliquer des politiques de sécurité strictes.
- Configurer les permissions des fichiers : s'assurer que les fichiers et répertoires sensibles ont des permissions appropriées (ex. : chmod, chown).
- Désactiver l'accès root à distance : interdire la connexion SSH en tant qu'utilisateur root en modifiant /etc/ssh/sshd_config.
- Utiliser des clés SSH : préférer l'authentification par clé SSH plutôt que par mot de passe pour les connexions SSH.
- Installer un logiciel antivirus : utiliser un logiciel antivirus pour détecter et prévenir les malwares.
- Configurer les journaux de sécurité : activer et surveiller les journaux de sécurité pour détecter les activités suspectes.
- Limiter les utilisateurs et groupes : restreindre les privilèges des utilisateurs et groupes, en appliquant le principe du moindre privilège.
- Activer le chiffrement des données : utiliser des systèmes de fichiers chiffrés pour protéger les données sensibles.
- Configurer des sauvegardes régulières : mettre en place un système de sauvegarde pour protéger les données contre la perte ou la corruption.

Zoomons sur SELinux afin de mieux comprendre son mode de fonctionnement. SELinux est un module de sécurité pour le noyau Linux qui fournit un mécanisme de contrôle d'accès basé sur des politiques. Il utilise des étiquettes de sécurité pour déterminer les permissions des processus et des fichiers, renforçant ainsi la sécurité du système en limitant les actions que les utilisateurs et les applications peuvent effectuer.

Prenons un exemple d'un process web (comme Apache ou NGINX) qui essaie d'accéder à un fichier de configuration. SELinux vérifie l'étiquette de sécurité du processus et celle du fichier. Si la politique permet cet accès, il est autorisé ; sinon, l'accès est refusé, protégeant ainsi le système contre les actions non autorisées. Il faudra donc ajuster la politique SELinux si vous souhaitez, et ceci est recommandé, configurer le serveur HTTP Apache pour qu'il écoute sur un port différent et pour qu'il fournisse du contenu dans un répertoire autre que celui par défaut.

Les règles de durcissement des environnements Windows ne sont pas fondamentalement différentes. Certains principes demeurent mais il existe des spécificités liées à l'OS cependant. Voir ci-dessous quelques exemples de règles à appliquer :

- Mise à jour régulière : activer Windows Update pour installer automatiquement les mises à jour de sécurité. La notion automatique est évidemment à adapter en fonction du contexte (station de travail ou serveur par exemple) et de la politique de sécurité. L'essentiel est que les mises à jour soient faites régulièrement et le plus tôt possible.
- Désactiver les services inutiles : identifier et désactiver les services non nécessaires via services.msc.
- Configurer un pare-feu : utiliser le pare-feu Windows pour contrôler le trafic réseau entrant et sortant.
- Utiliser des comptes utilisateurs standards : éviter d'utiliser des comptes administratifs pour les tâches quotidiennes.
- Activer l'UAC (Contrôle de compte d'utilisateur) : maintenir l'UAC activé pour limiter les privilèges des applications.
- Configurer les stratégies de mot de passe : appliquer des politiques de mot de passe strictes (longueur, complexité, expiration).

- Désactiver l'accès à distance non nécessaire : désactiver Remote Desktop si ce n'est pas utilisé, ou restreindre l'accès (interdire depuis Internet par exemple).
- Activer BitLocker : utiliser BitLocker pour chiffrer les disques durs et protéger les données.
- Installer un logiciel antivirus : utiliser un logiciel antivirus et maintenir ses définitions à jour.
- Configurer les journaux de sécurité : activer et surveiller les journaux d'événements pour détecter les activités suspectes.
- Désactiver SMBv1 : désactiver le protocole SMBv1 pour réduire les risques de vulnérabilités.
- Limiter les autorisations des applications : utiliser AppLocker ou Windows Defender Application Control pour contrôler les applications autorisées.

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. Pourquoi ? Tout simplement pour ne pas faciliter le travail des acteurs malveillants. Une simple recherche de vulnérabilités sur la version de votre composant exposé sur Internet peut en quelques secondes rendre clé en main un kit d'exploitation de cette vulnérabilité.

Au même titre que les OS et les applications, 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 SSHv2. 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, comme déjà énoncé, plusieurs règles précédemment citée doivent être utilisées. Il est indispensable 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 qui permettent des échanges chiffrés, tels que HTTPS, SMTPS et IMAPS, et d'utiliser des certificats valides pour garantir la sécurité des communications.

3.3 Hardware (HSM), Datacenter

Le durcissement et la sécurisation du matériel sont des éléments essentiels pour protéger les infrastructures informatiques. L'une des premières mesures à envisager est le chiffrement des données, qui permet de garantir la confidentialité et l'intégrité des informations sensibles, même en cas de compromission physique.

Les modules de sécurité matériels (HSM - Hardware Security Module) représentent une solution robuste pour la protection des secrets cryptographiques et des données sensibles. Ces dispositifs physiques, conçus avec des mécanismes anti-effraction, offrent un environnement hautement sécurisé pour le stockage et la gestion des clés cryptographiques, des certificats numériques et autres secrets. Les HSM assurent non seulement la protection physique des données, mais effectuent également les opérations cryptographiques critiques directement dans leur environnement sécurisé, évitant ainsi l'exposition des clés dans la mémoire du système hôte. Ils sont particulièrement utilisés dans les infrastructures à clés publiques (PKI) décrits dans le premier paragraphe de ce chapitre, les systèmes de paiement et les environnements nécessitant une conformité réglementaire stricte. Les HSM intègrent des mécanismes de contrôle d'accès, de journalisation des opérations et de sauvegarde sécurisée, garantissant ainsi l'intégrité et la disponibilité des secrets tout au long de leur cycle de vie.

Il est également recommandé de créer des zones matérielles dédiées, telles que des mémoires sécurisées ou des cartes dédiées, pour stocker des données critiques et des clés de chiffrement. Cela limite l'accès aux informations sensibles et réduit les risques d'exposition.

Les centres de données ou Datacenter en anglais, sont des batiments dédiés à l'hébergement de serveurs informatiques. Leur fonction impose naturellement un contrôle d'accès afin de restreindre l'entrée aux personnes autorisées uniquement. Leur sécurisation peut être assurée par l'utilisation de caméras de surveillance et la

présence de vigiles qui assureront la surveillance en temps réel des activités afin de réagir rapidement en cas d'incident.

3.4 Sécurisation des réseaux

La sécurisation et le durcissement des réseaux informatiques nécessitent une approche multicouche intégrant plusieurs niveaux de protection. Comme décrit dans le 3ème chapitre, la protection périmétrique constitue la première ligne de défense, s'appuyant sur des pare-feu nouvelle génération (NGFW) couplés à des systèmes de détection et de prévention d'intrusion (IDS/IPS).

Les réseaux de transit, particulièrement vulnérables aux attaques, requièrent une attention spécifique avec le déploiement de protocoles de chiffrement robustes comme TLS 1.3 et AES-256 (versions de en 2023-2024, ces protocoles évoluent et leur choix doit être en adéquation du besoin de la version disponible). La segmentation réseau, via l'utilisation de VLAN et de zones DMZ, ainsi que le filtrage du trafic par des listes de contrôle d'accès (ACL), renforcent cette protection.

Pour sécuriser les connexions distantes, les VPN intègrent une authentification forte reposant sur des certificats et l'authentification multifacteur (MFA), des tunnels IPsec ou SSL/TLS (cf. chapitre 3 également), ainsi qu'un chiffrement de bout en bout des communications.

Comme explicité et décrit plus précisement dans le chapitre X, les réseaux doivent être supervisés via un dispositif de monitoring continu assuré par des SIEM et des SOC, permettant la détection des anomalies et incidents.

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

4. Organisation de la sécurité dans les projets

La sécurité dans les projets est un aspect essentiel qui diffère de la sécurité globale de l'entreprise. Alors que la sécurité de l'entreprise se concentre sur la protection des actifs, des données et des infrastructures à un niveau macro, la sécurité dans les projets se concentre sur l'intégration de mesures de sécurité tout au long du cycle de vie d'un projet. Cela nécessite une collaboration étroite entre plusieurs équipes, notamment l'ingénierie, les opérations et le pilotage.

4.1 Ingénierie

L'équipe d'ingénierie est responsable de la conception et du développement des solutions. Elle doit intégrer des pratiques de sécurité dès le début du processus de développement, en effectuant des analyses de risques, en appliquant des normes de codage sécurisé et en réalisant des tests de sécurité.

Les Missions de ces équipes sont :

- **Analyse des risques** : identifier les vulnérabilités potentielles dès la phase de conception ;
- **Normes de développement sécurisé** : appliquer des pratiques de développement qui minimisent les risques de sécurité ;
- **Tests de sécurité** : effectuer des tests et des revues de code pour détecter et corriger les failles de sécurité ;
- **Documentation** : créer une documentation détaillée des mesures de sécurité intégrées dans le projet.

4.2 Opération

L'équipe des opérations gère l'implémentation et le déploiement des solutions. Elle doit s'assurer que les environnements de production sont sécurisés, en appliquant des mises à jour régulières et en surveillant les systèmes pour détecter toute activité suspecte. Les Missions de ces équipes sont :

- **Gestion des environnements** : Assurer que les environnements de développement, de test et de production sont sécurisés ;
- **Mises à Jour et correctifs** : appliquer régulièrement les mises à jour de sécurité et les correctifs pour corriger les vulnérabilités ;
- **Surveillance** : mettre en place des systèmes de surveillance pour détecter toute activité suspecte ou non autorisée ;
- **Réponse aux incidents** : développer et exécuter des plans de réponse aux incidents pour minimiser l'impact des incidents de sécurité.

4.3 Pilotage

L'équipe de pilotage supervise l'ensemble du projet et s'assure que les objectifs de sécurité sont respectés. Elle coordonne les efforts entre les équipes d'ingénierie et d'opérations, en établissant des indicateurs de performance et en réalisant des audits réguliers pour garantir la conformité aux politiques de sécurité.

Les Missions de ces équipes sont :

- **Coordination** : faciliter la communication et la collaboration entre les équipes d'ingénierie et des opérations ;
- **Indicateurs de performance** : établir des key performance indicator (KPI) pour mesurer l'efficacité des mesures de sécurité ;
- **Audits** : réaliser des audits réguliers pour garantir la conformité aux politiques de sécurité ;
- **Formation et sensibilisation** : organiser des sessions de formation pour sensibiliser les équipes aux meilleures pratiques en matière de sécurité.

- #Ingénierie, #opération, #pilotage
- #OrganisationSécurité

5. Sécurité des produits

La conformité technique aux référentiels et normes constitue un pilier essentiel pour garantir que les produits logiciels et matériels répondent aux exigences réglementaires et aux standards de sécurité de l'industrie. Cette démarche de conformité permet non seulement de valider la robustesse des solutions déployées mais aussi d'assurer leur interopérabilité et leur niveau de sécurité.

Ce chapitre présentera la conformité aux implementations normatives les plus connues ainsi que les dispositifs de certifications existants.

5.1 Conformité aux implémentations normatives

Pour aider à protéger les informations sensibles et les infrastructures critiques, divers référentiels ont été développés pour définir l'état de l'art en matière de sécurité informatique. Ces référentiels fournissent des cadres, des normes et des meilleures pratiques pour guider les organisations dans la mise en place de mesures de sécurité efficaces. Ce chapitre présente une liste ci-après de ces référentiels. Cette liste n'est évidemment pas exhaustive et est évolutive.

Il est à noter que la certification d'un périmètre ou système est aussi un atout concurrentiel majeur pour une entreprise. Une certification comme l'ISO/EIC 27001 témoigne de l'engagement de l'entreprise envers la protection des données et la gestion des risques, renforçant ainsi la confiance des clients et des partenaires. Par exemple, une entreprise de services financiers certifiée ISO 27001 peut se démarquer sur le marché en rassurant ses clients sur la sécurité de leurs informations sensibles, ce qui peut conduire à une fidélisation accrue et à l'acquisition de nouveaux clients, tout en minimisant les risques de violations de données.

5.1.1 ISO/IEC 27001

L'ISO/IEC 27001 est une norme internationale pour les systèmes de management de la sécurité de l'information (SMSI). Elle spécifie les exigences pour établir, mettre en œuvre, maintenir et améliorer continuellement un SMSI. C'est une norme qui sert de "livre de chevet" pour tous les dirigeants de la sécurité, RSSI ou directeur de la sécurité. Elle donne les bonnes pratiques de gouvernance ainsi que les mesures à appliquer pour contrôler la mise en oeuvre. Cette norme est certifiante pour les SMSI mais aussi pour les utilisateurs implémenteurs ou auditeurs.

5.1.2 NIST Cybersecurity Framework (CSF)

Le NIST Cybersecurity Framework (CSF) est un cadre développé par le National Institute of Standards and Technology (NIST) pour améliorer la gestion des risques de cybersécurité. Il se compose de cinq fonctions principales : Identifier, Protéger, Détecter, Répondre et Récupérer. De très nombreux documents ont été édités par le NIST et servent aux organisations et responsables.

5.1.3 CIS Controls

Les CIS Controls sont un ensemble de 20 contrôles de sécurité critiques publiés par le Center for Internet Security (CIS). Ils sont conçus pour aider les organisations à se défendre contre les cybermenaces les plus courantes. Cf. chapitre 6.2 pour plus d'information sur l'application et l'utilisation de ces controles.

5.1.4 COBIT

Le COBIT est un Framework de gouvernance et de management des technologies de l'information (TI) développé par ISACA. Il fournit des outils pour aligner les objectifs de l'entreprise avec les objectifs de la TI.

5.1.5 PCI DSS

La norme PCI DSS est une norme de sécurité des données pour l'industrie des cartes de paiement. Elle vise à protéger les informations des titulaires de carte et à réduire la fraude liée aux cartes de paiement.

5.1.6 GDPR

Le Règlement général sur la protection des données de l'Union européenne (ou GDPR en anglais pour General Data Protection Regulation) impose des obligations strictes aux organisations qui collectent ou traitent des données personnelles de résidents de l'UE.

5.1.7 HIPAA

l'HIPAA (Health Insurance Portability and Accountability Act) est une loi américaine sur la portabilité et la responsabilité en matière d'assurance maladie. Elle établit des normes pour la protection des informations de santé des patients.

5.1.8 SOC 2

La norme Service Organization Controls 2 (SOC 2) est une norme de conformité pour les organisations de services. Elle se concentre sur les contrôles relatifs à la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité et la vie privée.

5.1.9 OWASP Top Ten

Le top 10 OWASP est liste des dix principales vulnérabilités de sécurité des applications web, publiée par l'Open Web Application Security Project (OWASP). Elle sert de guide pour les développeurs et les professionnels de la sécurité.

5.1.10 ITIL

L'Information Technology Infrastructure Library (ITIL) est une bibliothèque pour l'infrastructure des technologies de l'information. Elle fournit un ensemble de processus des meilleures pratiques pour la gestion des services informatiques, y compris la gestion de la sécurité de l'information.

5.1.11 SANS Top 20

Le top 20 publié par SANS Institute liste les 20 contrôles de sécurité critiques conçus pour aider les organisations à se protéger contre les cybermenaces les plus courantes.

5.1.12 CSA CCM

Le Cloud Controls Matrix (CCM) est un cadre de contrôle de la cybersécurité pour le cloud, publiée par la Cloud Security Alliance (CSA). Elle fournit des recommandations pour sécuriser les environnements de cloud computing.

5.1.13 ISO/IEC 27017

La norme ISO/IEC 27017 donne un code de pratique pour les contrôles de sécurité de l'information basés sur ISO/IEC 27002 pour les services cloud. Elle fournit des lignes directrices spécifiques pour les fournisseurs de services cloud.

5.1.14 ISO/IEC 27018

La norme ISO/IEC 27018 donne un code de pratique pour la protection des informations personnelles (PII) dans les services cloud publics. Elle se concentre sur la protection des données personnelles dans les environnements de cloud computing.

5.1.15 ENISA

L'Agence de l'Union européenne pour la cybersécurité publie des lignes directrices et des recommandations pour améliorer la cybersécurité en Europe. Elle fournit des ressources pour aider les organisations à se protéger contre les cybermenaces. Par exemple, on peut citer le texte sur la sécurité de la 5G.

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.

Quel est l'intérêt de ce type de certification ?

Pour le vendeur :

- confiance accrue : la certification CSPN renforce la crédibilité du produit auprès des clients potentiels ;
- avantage concurrentiel : se démarquer sur le marché en offrant des produits reconnus pour leur sécurité ;
- accès à de nouveaux marchés : facilite l'entrée sur des marchés sensibles où la sécurité est primordiale.

Pour l'acheteur :

- garantie de sécurité : assurance que le produit a été évalué et répond à des normes de sécurité élevées ;
- réduction des risques : diminution des vulnérabilités potentielles dans l'infrastructure de l'entreprise ;
- conformité réglementaire : aide à respecter les exigences légales et réglementaires en matière de sécurité des systèmes d'information.

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 leur site. (source ANSSI)

Plusieurs produits dont les fonctionnalités ont été décrites dans le chapitre 3 sont certifiés CSPN, les EDR Harfanglab ou la suite logicielle de sécurisation du poste de travail de Stormshield [4].

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) Les produits utilisés pour chiffrer des documents, des emails voire des postes de travail comme Zed ! et ZoneCentral de PRIM'X sont par exemples certifiés critères communs [5]

- Conformité == répondre aux exigences réglementaires et aux standards de sécurité de l'industrie

  –> #ISO/IEC 27001 #NIST #CIS Controls #COBIT #PCI DSS #GDPR –> #HIPAA #SOC 2 #OWASP Top Ten #ITIL #SANS Top20 #CSA CCM –> #ISO/IEC 27017 #ISO/IEC 27018 #ENISA
- La confiance certifié

  –> #CSPN #Critères Communs

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

7. Règles techniques de sécurisation et durcissement

7.1 Sécurisation des systèmes d'exploitation

7.1.1 Mise à jour et gestion des correctifs

7.1.2 Configuration des paramètres de sécurité

4. liste des produits certifiés ANSSI CSPN : https://cyber.gouv.fr/produits-certifies ?sort_bef_combine=field_date_de_certification_value_-DESCtype_1%5Bproduit_certifie_cspn%5D=produit_certifie_cspn
5. liste des produits certifiés ANSSI CC : https://cyber.gouv.fr/produits-certifies ?sort_bef_combine=field_date_de_certification_value_-DESCtype_1%5Bproduit_certifie_cc%5D=produit_certifie_ccfield_categorie_target_id%5B536%5D=536field_categorie_target_-id%5B534%5D=534

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