SEC105 - Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications

PEI Millau – Concepteur Architecte Informatique (toutes spécialités)

Objectif : Comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de sécurité, expliquer DICT, la différence avec la sureté de fonctionnement, mettre en place les mesures de base sur tout système, OS.

Thème : ***Sécurité de base des matériels et systèmes d'exploitation***

Commençons par le début : le MCS

Définition :

Le MCS (Maintien en Condition de Sécurité) a pour objectif *d'assurer le niveau de sécurité d'un système* ou d'un projet *durant toutes les phases de son cycle de vie* au travers d'une *gestion maîtrisée et pérenne des risques* liés aux *vulnérabilités* logicielles.

À ce titre, le MCS est présenté comme indispensable dans la *Politique de sécurité des systèmes d'information (PSSI),* qui fixe les règles de protection applicables aux SI.

Il s'agit d'une *démarche* visant à collecter, agréger et synthétiser les informations traitant des évolutions de la menace et des vulnérabilités.

Il s'agit également de *qualifier* le risque dans le temps et, bien entendu, de décider des actions à faire par rapport à ce risque :

- l'accepter,
- le réduire,
- le transférer
- l'annuler.

En pratique, cela se traduit souvent techniquement par un déploiement de correctifs de sécurité, aux différents niveaux considérés pour le maintien en condition.

MCS vs. Sureté de fonctionnement

À ce titre, le MCS se distingue de la sureté de fonctionnement par le fait qu'il engage une démarche bien **plus globale** de la gestion des risques de sécurité, là où la sureté de fonctionnement se focalise sur l'aptitude d'un système à remplir une ou plusieurs fonctions requises dans des conditions données.

La sureté de fonctionnement englobe quatre composantes :

- **la fiabilité,**
- **la maintenabilité,**
- **la disponibilité**
- **et la sécurité**.

MCS – Approche globale

Le MCS est une approche globale qui se doit d'être porté par tous les collaborateurs, sous la responsabilité de la direction des systèmes d'information ou du RSSI (Responsable de la Sécurité des Systèmes d'Information).

Traditionnellement, elle s'opère de manière progressive et participative, afin d'atteindre les objectifs fixés par la PSSI * :

- **Prendre connaissance de son SI** en réalisant une cartographie en priorisant les éléments les plus critiques ;
- **Mitiger les risques sur le SI** en mettant en place l'état de l'art de l'architecture réseau sécurisée et définir les processus d'administration – les SI de Sûreté, par leur criticité, devront faire l'objet d'une attention particulière ;
- **Atteindre un niveau de sécurité adéquat** par le durcissement et le maintien en conditions de sécurité des équipements dans le temps – des discussions pourront notamment avoir lieu avec les fournisseurs et constructeurs d'équipements ;
- **Mettre en place les outils nécessaires à la détection d'incident de sécurité**, qui peuvent avoir une influence sur la production, et définir les processus de réaction.

Notez que tout ce que nous avons vu précédemment peut entrer soit dans la démarche (ISO2700x, PSSI, analyse du risque etc.), soit dans les outils (PCA, Plan de continuité d'activité, PRA , Plan de reprise d'activité, etc.)

* *Politique de sécurité des systèmes d'information*

MCS – Prendre connaissance de son SI

Cette première étape est déterminante, et peut s'effectuer dans un contexte plus rigoureux lié à des objectifs qualité (ISO27001).

Dans tous les cas, elle est le point de départ pour une bonne gouvernance de la sécurité.

Objectifs :

- Pouvoir apprécier l'impact d'une compromission.
- Faciliter le traitement des incidents de sécurité.
- Pouvoir qualifier et attribuer des signalements remontés.

PSSI & Cartographie

MCS – Mitiger les risques sur le SI

Ne pas négliger le fait que notre SI communique par le réseau : il est alors important de l'inclure afin d'assurer une bonne gouvernance.

Objectif :

- Pouvoir maitriser les flux de données qui doivent transiter au sein du SI (cartographie) ;
- Adapter les besoins de communication en choisissant les protocoles les plus adaptés à la sécurisation des flux de données ;
- Gérer les risques liés aux infrastructures de télécommunication ;
- Mettre en œuvre et maintenir une infrastructure de communication facilitante ;
- Pouvoir qualifier et attribuer des signalements remontés.

Gestion des identités & accès.
Administration.
Défense en profondeur.

MCS – Atteindre un niveau de sécurité adéquat

Cette étape a pour but de définir une trajectoire et des processus visant à maintenir un niveau de sécurité au niveau des équipements du SI.

Selon l'actif et son niveau de criticité pour le SI, des processus d'exploitation, de maintenance et de gestion des incidents de sécurités peuvent venir enrichir notre démarche.

Objectif :

- Durcir les actifs du SI de manière à assurer un niveau de sécurité maitrisé, tout en ne dégradant pas leur capacité à tenir leur rôle ;
- Être le support de suivi du cycle de vie de ces actifs ;
  Pouvoir qualifier et attribuer des signalements remontés.

Nous reviendrons plus tard sur les bonnes pratiques relatives aux systèmes d'exploitation.

Gestion des identités & accès.
Administration.
Défense en profondeur.

MCS – Mettre en place les moyens de gestion des incidents de sécurité.

Cette dernière étape repose bien entendu sur les trois précédentes.

Objectif :

- Être acteur du processus de gestion des incidents de sécurité ;
- Se doter de moyens fiables et maitrisés permettant d'identifier des incidents de sécurité ;
- Mettre en œuvre des processus en réponse à ces incidents, tenant compte de leur impact, de leur gravité et du périmètre.

Journalisation.
Détection.
Traitement des incidents de sécurité.
Traitement des alertes.

Mise en place de mesures : Matériel

EXIGENCES DE SÉCURITÉ MATÉRIELLE POUR PLATE-FORMES X86 [GUIDE ANSSI]

Pour la maitrise de la plate-forme matériel :

- Inventaire matériel exact (liste composants livrés vs composants installés.)
- Pouvoir démonter le matériel inutile (ex. Interfaces sans-fil)
- Non dépendance Matériel / OS

Exigences concernant les caractéristiques matériel :

- Disposer d'une I/OMMU * active ➔ Protection de la mémoire centrale
- Si présence d'un TPM (*Trusted Platform Module*), s'assurer de sa robustesse et de sa conformité.

* *IOMMU ou I/OMMU : input–output memory management unit. VT-d, Virtualization Technology for Directed I/O, chez Intel.*

Mise en place de mesures : Matériel

EXIGENCES DE SÉCURITÉ MATÉRIELLE POUR PLATE-FORMES X86 [GUIDE ANSSI]

Exigences firmware :

- *Firmware* configurable : mot de passe, désactivation de périphériques, paramétrage du *SecureBoot*, protection de l'accès à l'interface de paramétrage.
- Caractérisation du niveau de sécurité des *firmwares*
- Désactivation des options d'assistance à distance
- Les mécanismes de protection contre l'inspection de code doivent soit être absents du *firmware*, soit être désactivés par défaut

Pour le MCS :

- Fournitures de correctifs
- Application des correctifs

Mise en place de mesures : OS

EXIGENCES DE SÉCURITÉ MATÉRIELLE POUR PLATE-FORMES X86
[GUIDE ANSSI]

Principes généraux :

- **Minimisation** : n'installer que ce qui est absolument nécessaire
- **Moindre privilège :** tout objet ou entité du système ne dispose que des droits nécessaires + mise en place d'un contrôle d'accès adapté.
- **Défense en profondeur (quand nécessaire)** : Authentification / journalisation / cloisonnement + séparation des privilèges / mécanismes de prévention d'exploitation
- **Veille et maintenance** : journalisation des activités, mises à jour régulières

Mise en place de mesures : OS

RECOMMANDATIONS DE CONFIGURATION D'UN SYSTÈME GNU/LINUX [GUIDE ANSSI]

Installation du système :

- **Partitionnement adapté :** partitionnement adapté à l'usage, isolation des composantes du système, options de montage adaptés (ex. W^X ou W xor X)
- **Installation des paquets :** réduits au strict nécessaire, dépôts de confiance, voir paquets durcis
- **Configuration du chargeur de démarrage :** mot de passe, activation de l'I/OMMU …
- **Mots de passe : utilisation de mot de passe pour les comptes à privilèges et les comptes utilisateurs**
- **Utilisation de moyens cryptographiques**

Mise en place de mesures : OS

RECOMMANDATIONS DE CONFIGURATION D'UN SYSTÈME GNU/LINUX [GUIDE ANSSI]

Configuration & services :

- **Services exposés :** attention aux flux non maitrisés, privilégier les services durcis ou à défaut les surveiller.
- **Configuration du système :** paramétrage fin en rapport avec le besoin (mémoire, réseau, noyau etc…) – sysctl
- **Gestion des utilisateurs renforcée :** désactivation des comptes non utilisés, exclusivité des comptes de services, expiration des comptes.
- **Configuration adaptés des modules d'authentification et d'accès aux données administratives**
- **Gestion des droits :** utilisation d'une politique et de commandes adaptées, avec attention particulière sur certains « flags » spécifiques (SetUID)
- **Configuration du système de journalisation**
- **Configuration de certains services sensibles (mails etc…)**
- **Mise en place de services d'audit** (auditd)
- **Surveillance des systèmes de fichiers :** vérification des modifications …

Mise en place de mesures : OS

RECOMMANDATIONS DE CONFIGURATION D'UN SYSTÈME GNU/LINUX [GUIDE ANSSI]

Cloisonnement & contrôle d'accès :

- **Utilisation d'outils adaptés : chroot, etc..**
- **Application d'une politique et d'un outil de contrôle d'accès :** AppArmor, SELinux, mais aussi des outils d'élévation de droits comme sudo

Niveau	Description
M I R E	Recommandation de niveau **minimal**. À mettre en œuvre systématiquement sur tout système.
I R E	Recommandation à appliquer dès le niveau **intermédiaire**. Correspond généralement à des services protégés par plusieurs couches de sécurité de niveau supérieur.
R E	Recommandation s'appliquant dès le niveau **renforcé**. Généralement pour des systèmes exposés à des flux non authentifiés ou de sources nombreuses.
E	Recommandation valide au niveau **élevé**. Correspond à des systèmes hébergeant des données sensibles accessibles depuis des réseaux non authentifiés ou peu contrôlés.

TABLE 2.1 – Grille de lecture des niveaux de durcissement

L'objectif étant d'arriver à un niveau de durcissement adapté et maîtrisé.

Mise en place de mesures : OS

Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows [NOTE ANSSI]

Mécanismes de restriction applicatives (Software Restriction Policies / AppLocker) :

- **Maitriser les logiciels installés**
- **Mise en place d'outils et de politiques adaptées**
- **Définition d'une politique de restriction adaptée.**
- **Démarche d'audit / réévaluation régulière** ➔ amélioration continue.

On peut ajouter toutes les règles élémentaires du guide d'hygiène informatique : Chiffrer les volumes ou les données sensible, utiliser des logiciels éprouvés, mettre en œuvre la cryptographie, etc…

Notez également que pour Windows 10, l'ANSSI à édité un guide nommé « Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10 »