Fiche de révision I43 Essentielle

Sommaire :

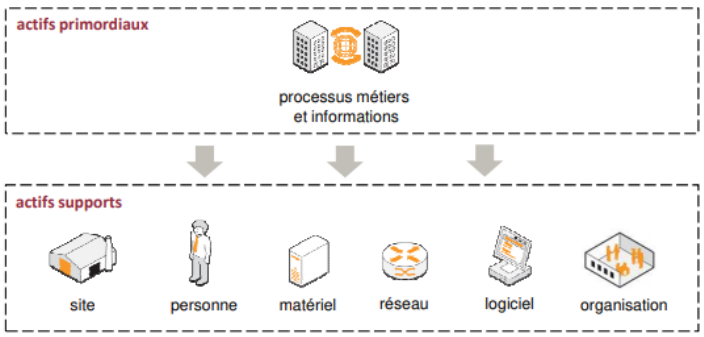
Module 1 :

-Définition S.I : On appelle système d'information un ensemble de ressource destinée à collecter, classifier, stocker, gérer diffuser les **informations** au sein d'une organisation.

Norme ISO/IEC 27005 :2008

-Actif primordiaux : Les information de l'entreprise et son savoir-faire

-Actif support : Le site physique, le matérielle, personne, réseaux, logicielle, organisation.



-La gestion de la sécurité a pour but de contribue à la qualité service des utilisateurs et garanti la protection du personnelle.

-Un opérateur d'importance vitale (OIV) est, en France, une organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation[1] ou dangereuses pour la population.

D.I.C = disponibilité, intégrité, Confidentialité

- 3 critères sont retenus pour répondre à cette problématique, connus sous le nom de D.I.C.

Bien à protéger

Disponibilité
Propriété d'accessibilité au moment voulu des biens par les personnes autorisées (i.e. le bien doit être disponible durant les plages d'utilisation prévues)

Intégrité
Propriété d'exactitude et de complétude des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)

Confidentialité
Propriété des biens de n'être accessibles qu'aux personnes autorisées

+**Preuve** : traçabilité des action menée, authentification, imputabilité.

Sureté : Protection contre les **Actions involontaires**
Sécurité : protection contre les **Actions malveillantes volontaire**

Sûreté : ensemble de mécanismes mis en place pour assurer la continuité de fonctionnement du système dans les conditions requises.

Sécurité : ensemble de mécanismes destinés à protéger l'information des utilisateurs ou processus n'ayant pas l'autorisation de la manipuler et d'assurer les accès autorisés.

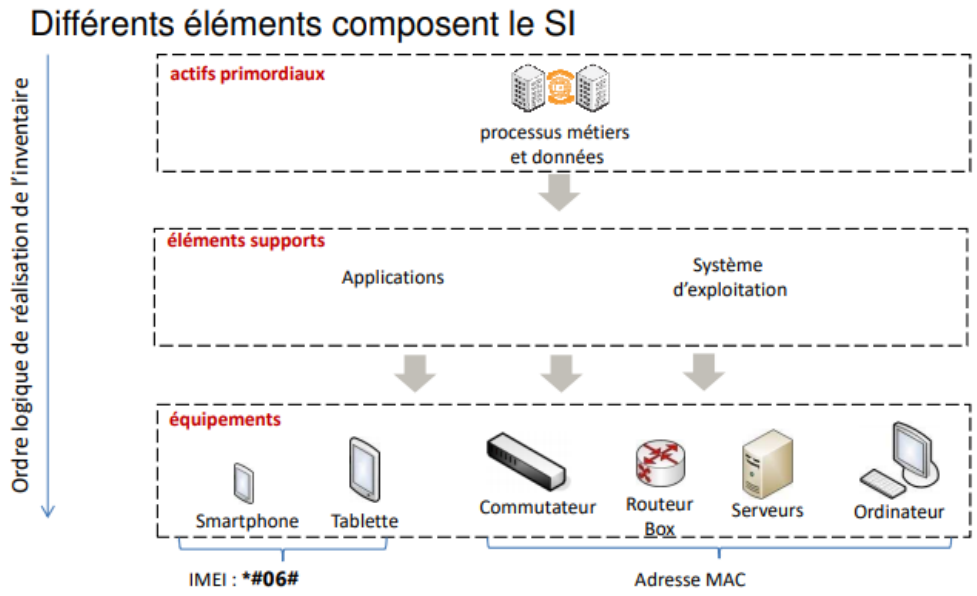
Vulnérabilité : Faiblesse au niveaux d'un bien
Menace : Cause potentielle d'un incident
Attaque : Action malveillante destinée à porter atteinte à un bien, Elle représente la concrétisation d'une *menace* et nécessite une *vulnérabilité*

Définition de la cybercriminalité :
Ensemble des actes contrevenants aux traités internationaux ou aux lois nationales utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Définition de l'investigation numérique *(forensics)* :
Ensemble des protocoles et de mesures permettant de rechercher des éléments techniques sur un conteneur de données numériques en vue de répondre à un objectif technique en respectant une procédure de préservation du conteneur.

Probablement inutile

Module 2 :



L'inventaire des biens doit suivre une **méthodologie logique**, afin d'être exhaustif, en commençant par l'inventaire des métiers

RESEAUX : **Tout ce qui n'est pas explicitement autoriser est interdit** (white list not black list).

B.Y.O.D c'est pas bien, votre pc est une vulnérabilité. Mettre à jour la base virale si !

Principe important sur les utilisateurs :

Moindre privilège, N'attribuer que le minimum de privilège nécessaire.

Besoin d'en connaitre, restreindre l'accès au répertoire sensible, et donner l'accès uniquement au donné nécessaire.

1 utilisateur = 1 compte

Pour gérer tout ça il existe 3 admin :

- Administrateur système : en charge de l'administration des systèmes, de la gestion des disques ;
- Administrateur réseau : en charge des équipements réseaux, des règles de filtrage ;
- Administrateur sécurité : en charge de la journalisation, de la supervision.

De préférence les rôles d'administrateurs système et sécurité doivent être donnés a des personnes différentes

Un audit permet d'évaluer le niveau de Sécurité, obtenir une certification
Trouver des failles.
Il existe aussi 4 type audit :
Boite noir(pentest) : aucun accès
Boite grise (test du stagiaire) : on Dispose de peu d'info et on essaye D'élever les privilèges
Boite blanche : on est root **Forensic** : après attaque

Module 3 :

Le **protocole ip** et les protocole associé(TCP,UDP.ICMP,routage) ne possède aucun mécanisme interne les permettant d'être **sécuriser.**

Ainsi afin d'obtenir un niveau de sécurité suffisante il **faut** :
-chiffrement de communication
-cloisonnement du réseau
-authentifier les entités
-filtrage

Quelques exemples de faiblesses de ces protocoles

- **Absence d'authentification des émetteurs et récepteurs** d'un datagramme : usurpation d'adresse IP possible ;
- **Absence de chiffrement des données**, celles-ci sont donc transmises en clair. Un hacker positionné sur un réseau peut donc écouter les connexions et accéder aux données ;
- **Le routage des datagrammes peut être modifié** de façon à rediriger les datagrammes vers un autre destinataire ;
- Note : l'exploitation de ces faiblesses nécessite des prérequis techniques, i.e. elles ne sont pas systématiquement applicables à tous les réseaux.

IDS Alert pas de coupure**/IPS** bloque donc coupure

V.P.N Tunnel virtuelle chiffrer avec une garanti d'intégrité.

La segmentation c'est important. (vlan)

D.M.Z : Une dmz(zone démilitarisé) est une zone réseaux destinée a isoler le web du réseaux interne.

Proxy : Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.

Proxy inverse : permet à un utilisateur d'Internet d'accéder à des serveurs internes.

Crypto : Intégrité, Confidentialité, Preuve (le reste est vue avec le DOSSO)

Attaque par injection :
En bref : Il s'agit d'une attaque qui utilise une faille de la base donnée afin d'interagir directement avec elle
Protection : Respecter les bonne pratique de développement ('prepared statement')

Usurpation cookie :
En bref : Il s'agit de récupère les cookie afin de se faire passer pour qu'elle qu'un d'autre
Protection : HTTPS, sensibilisation, système ajour.

Module 4 :

Les Norme iso 27k Sont des norme de sécurité international

27001	• Systèmes de management de la sécurité de l'information
27002	• Code de bonnes pratiques
27004	• Mesures du management de la sécurité
27005	• Gestion des risques
27035	• Gestion des incidents de sécurité
27037	• Traitement des preuves numériques *(forensics)*
...	• ...

Norme iso 27001 : Il s'agit de la norme de certification.
Norme iso 27002 : définie **les bons pratiques** en matière de cyber, Cette norme possède un référentielle de mise en œuvre ainsi que d'une check List pour les audits.
Norme iso 27005 : Liste de **ligne directrice(**démarche**)** concernant la sécurité

La certification 2700 n'indique pas un niveau de sécurité minimal, Une entreprise peut être certifier et tout nul

Liste des phases de la norme 27001 :

-Phase plan : fixer les objectif et le plan d'action
-Phase do : mise en œuvre
-phase check : vérification après un délai (1 ans par exemple
-phase acte : Conclusion de la phase check, correction des problèmes

La norme ne dure que 3 ans.

Relation humaine :
Avant embauche :
-vérification cv/casier judiciaire
Apres embauche :
-Sensibilisation sécurité
-fourniture des accès nécessaire
Départ :
-retrait des accès et restitution Du matérielle.

Classification des information

	Intitulé	Explication
C1	Accès libre	Tout le monde peut y accéder
C2	Accès à l'organisation	Seul le personnel de l'organisation est autorisé à accéder à l'information
C3	Diffusion limitée	Au sein de l'organisation, seul un groupe de personnes est autorisé comme les membres du même projet
C4	Confidentiel	L'information est accessible à une liste très restreinte d'utilisateurs à titre individuel

La sécurité doit être pris en charge dans toute les étapes du projet

L'analyse de risques doit être effectuée en amont du projet mais doit aussi évoluer au fur et à mesure de celui-ci et fonction de l'évolution des risques.

Cette analyse consiste à :

- -identifier les bien à protéger.
- -analyse la dangerosité des menaces.
- -définir les priorités
- -définir les mesures mettre en place.

Le **shadow IT** est le fait d'utiliser un un saas(software as service) par un employé sans l'aval de son employeur il s'agit d'une faille de sécurité.(pour se protéger on utiliser un acces Security broker)

Le big data *peut*-être une opportunité.

La cyber embauche…