UTC505 Introduction à la Cyberstructure de l'internet : réseaux et sécurité

Séance 1
Concepts généraux
De sécurité

Cnam de Lille - Auteur : Jérémy Merlin

Table des matières

1. Sécurité définition (*)

Physiquement, la **sécurité** est l'état d'une situation présentant le minimum de risque.

Psychiquement, la **sécurité** est l'état d'esprit d'une personne qui se sent tranquille et confiante. Pour l'individu ou un groupe, c'est le sentiment (bien ou mal fondé) d'être à l'abri de tout danger et risque.

La sécurité est un concept applicable à de nombreux domaines comme par exemple :

- La défense
- La sécurité nationale
- La sécurité économique
- La sécurité alimentaire

Lorsque l'on parle de la sécurité des systèmes d'information, on fait référence

aux politiques et procédures qui permettent d'éviter les intrusions (confidentialité), les incohérences (intégrité) et les pannes (disponibilité) des systèmes d'information, et qui définissent les règles d'authentification.

La sécurité des systèmes d'information est un domaine particulièrement stratégique de la sécurité, car, à travers les systèmes de contrôle, les systèmes de gestion, et d'une façon générale à travers l'ingénierie des systèmes, elle doit s'intéresser à l'interopérabilité des systèmes, et faire en sorte que la sécurité soit obtenue au travers de standards et de normes de description des structures de données.

On parle aussi de sécurité informatique (terme plutôt ancien utilisé pour des ordinateurs et systèmes moins répartis) et plus récemment de sécurité de l'information notamment parce que l'on souhaite étendre la notion de protection de l'information au-delà des pures systèmes (comportements humaines, documents papiers etc…).

Plus spécifiquement la sécurité des réseaux concerne une sous-parties de la sécurité des systèmes d'informations concernant les couches de transport de cette information sur les réseaux informatiques.

`* source : Wikipedia.

2. Les 6 axes de la sécurité

1.1. Quatre axes majeurs

- la **disponibilité**

- l'**intégrité** d'un objet (document, fichier, message …) est la garantie que cet objet n'a pas été modifié par une autre personne que son auteur.

- la **confidentialité** est l'assurance qu'un document ne sera pas lu par un tiers qui n'en a pas le droit lors de la transmission de ce document ou lorsqu'il est archivé.

- la **traçabilité** est la capacité à identifier les différentes actions réalisées par et/ou sur le système

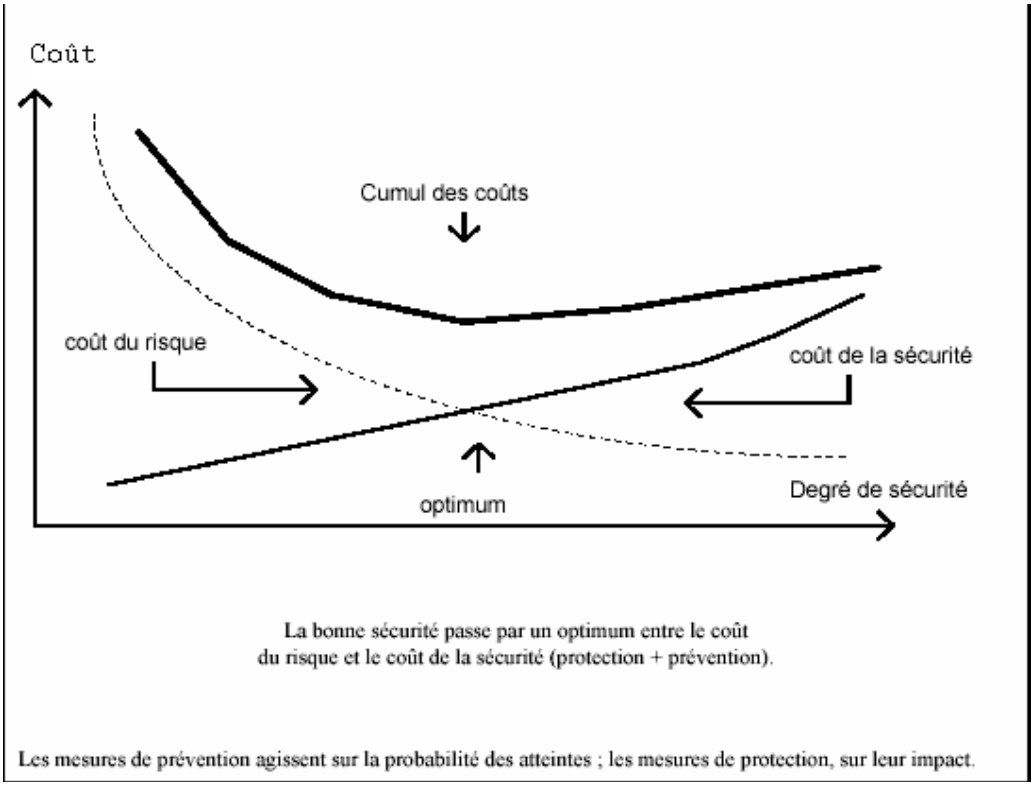
1.2. Et deux autres en découlant

- l'**authentification** est l'assurance de l'identité d'un objet, généralement une personne, mais cela peut aussi s'appliquer à un serveur, une application, …

- « **non répudiation »** est le fait que l'émetteur d'un message ne puisse pas nier l'avoir envoyé et le récepteur l'avoir reçu. Les transactions commerciales ont absolument besoin de cette fonction.

3. Recherche du point d'équilibre

- Respecter la réglementation
- Diminuer les risques à l'optimum



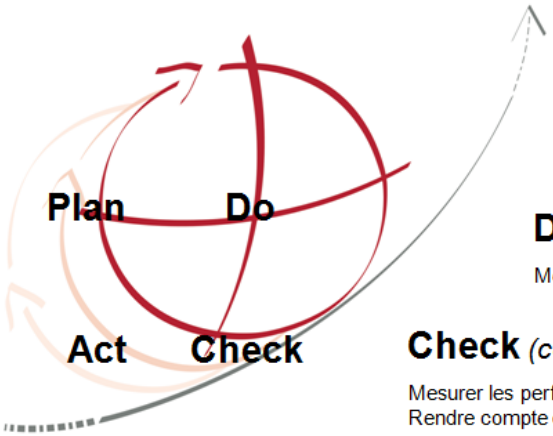
La bonne sécurité passe par un optimum entre le coût du risque et le coût de la sécurité (protection + prévention).

Les mesures de prévention agissent sur la probabilité des atteintes ; les mesures de protection, sur leur impact.

4. La sécurité globale de l'entreprise

5. La démarche de progrès permanent

Norme ISO 27001



Plan *(planifier)*

Définir le Référentiel ou la Politique de sécurité.
Mesurer la situation actuelle.
Établir les priorités et planifier les actions.

Do *(réaliser)*

Mettre en œuvre et exploiter le SMSI.

Check *(contrôler)*

Mesurer les performances du SMSI par rapport au référentiel défini.
Rendre compte des résultats.

Act *(décider)*

Décider de mesures correctives et préventives pour améliorer le SMSI.
Revoir le SMSI.

L'origine

La nouvelle norme internationale ISO 27001, publiée fin 2005, spécifie les processus qui permettent à une entreprise **d'établir, de mettre en œuvre et d'exploiter, de surveiller et de revoir, de maintenir et d'actualiser** un Système de Management de la Sécurité de l'Information.

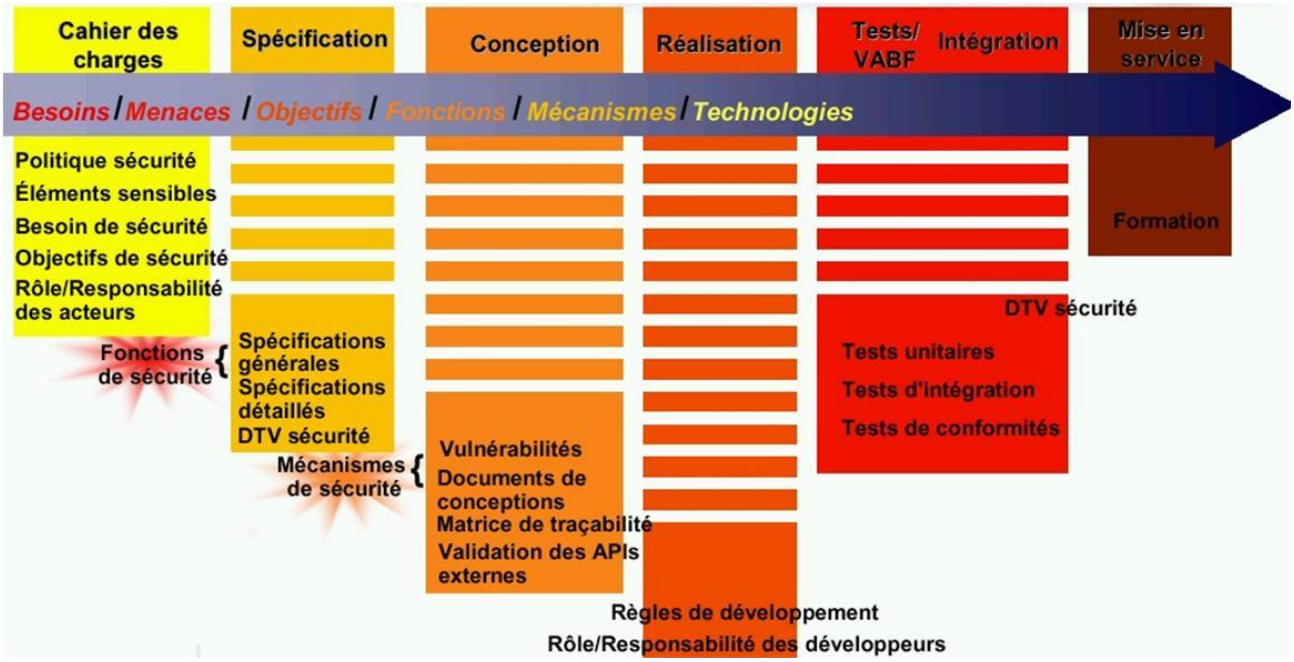
Elle intègre l'approche par processus des normes ISO relatives aux systèmes de management (ISO 9001 et ISO 14001), en particulier le cycle PDCA et l'exigence d'une **amélioration continue**.

La méthode "PDCA" est également appelée roue de l'amélioration de la qualité ou roue de Deming, du nom de W. Edwards DEMING, statisticien et philosophe américain.

Sécurité et processus projet

6. Sécurité et processus projet

5.1. Projets cycle en V



DTV = Dossier de Test et Validation

- **phase expression de besoin** : les utilisateurs doivent se positionnement sur des niveaux de sécurité attendus (Disponibilité, Intégrité, Confidentialité, Traçabilité)
- **spécifications fonctionnelles générales** : traduire cela en fonctionnalités de sécurité à mettre en œuvre de manière globale (redondances, sauvegardes, gestions des droits, mots de passe, traces et logs, doubles vérifications et contrôles).
- **spécifications fonctionnelles détaillées** : on rentre dans le détail de ces fonctions
- **spécifications techniques détaillées** : comment on met en œuvre
- **recette** : on vérifie que ce que l'on a dit que l'on allait faire dans les SFG est mis en œuvre correctement

- **mise en production** : règles de prudence, procédures de retour arrière, dossiers d'exploitation
- **maintenance** : mise à jour des systèmes, nouvelles failles, gestions des habilitations.

5.2. Projets Agile

Les aspects de sécurité peuvent être pris en compte également dans les projets Agile mais de manière différente

- Expression de besoin : en alimentation de la backlog et des story Agile
- Spécifications : en partie en sprint 0 ou phase archi avant projet puis dans les sprints
- Recette et mises en production : inclus dans les sprints en mode CI/CD (Continuous Integration Continuous Delivery).

7. Sécurité et réseaux

7.1. Réseaux informatiques (*)

Un **réseau informatique** (en anglais, *data communication network* ou *DCN*) est un ensemble d'équipements reliés entre eux pour échanger des informations. Par analogie avec un filet (un réseau est un « petit rets », c'est-à-dire un petit filet[1]), on appelle nœud l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions ou équipements (un ordinateur, un routeur, un concentrateur, un commutateur).

Indépendamment de la technologie sous-jacente, on porte généralement une vue matricielle sur ce qu'est un réseau.

De façon *horizontale*, un réseau est une strate de trois couches : les infrastructures, les fonctions de contrôle et de commande, les services rendus à l'utilisateur. De façon *verticale*, on utilise souvent un découpage géographique : réseau local, réseau d'accès et réseau d'interconnexion.

`* source Wikipedia

7.2. Sécurité des réseaux

La sécurité des réseaux est une composante importante de la sécurité des Systèmes d'information :

- D'abord parce que les réseaux sont au cœur des échanges d'information et la croissance des flux est exponentielle depuis l'avènement d'Internet et dernièrement de l'Internet des objets

- La plupart des attaques sur le SI se font à distance, via les réseaux (Internet ou par rebond via des interconnexion de partenaires).

Sécuriser les réseaux est en soit un vaste chantier et il s'agit à la fois de :

- Sécuriser physiquement les équipements et les supports de transmission
- Sécuriser logiquement ces équipements contre les accès inappropriés et frauduleux en gérant les mots de passes, les habilitations ou encore en corrigeant les failles de ces équipements par exemple
- Il s'agit aussi de gérer la sécurité des flux d'informations qui circulent au travers de ces réseaux en créant diverses zones avec des niveaux de confiance, en vérifiant les destinataires, en chiffrant certains flux.
- Enfin la sécurité des réseaux repose aussi sur la sécurité des protocoles utilisés pour les emprunter.

Finalement la sécurité des réseaux peut totalement s'inscrire dans la gestion plus large de la sécurité de l'information d'une méthodologie ISO27001/27002 en la déclinant sur les aspects spécifiques dédiés aux réseaux.