PARTIE I

Sécurité du Système d'Information et Gestion des Risques

Introduction

- La sécurité du système d'information et la gestion des risques sont étroitement imbriqués.

- C'est en fonction d'une **analyse des risques** que seront mises en œuvre des **mesures de sécurité** destinées à réduire les risques à un niveau acceptable tel que défini par la **politique de sécurité**.

Information = élément stratégique

- **L'information** est un **actif** qui, comme d'autres actifs importants d'une organisation, représente une **valeur** pour celle-ci et de ce fait nécessite une **protection adéquate.**
- L'information existe sous de nombreuses **formes** :
  - Imprimée ou écrite sur du papier
  - Stockée électroniquement
  - Transmise par la poste ou des moyens électroniques
  - Visuelle, par exemple des vidéos ou des schémas
  - Publiée sur le Web
  - Verbale/orale, par exemple des conversations, des appels téléphoniques
  - Intangible, par exemple du savoir-faire, de la connaissance, de l'expérience, de l'expertise, des idées, etc.

*« Toutes les informations **détenues** et **traitées** par une organisation sont exposées à des **menaces d'attaque**, **d'erreur**, **d'événement naturel** (par exemple inondation ou incendie), etc. et sont exposées à des **vulnérabilités** inhérentes à leur utilisation.*

*Le terme **sécurité de l'information** repose, en général, sur le fait que l'information est considérée comme un **actif** qui a une **valeur** et qui, en tant que tel, nécessite une **protection appropriée** contre, par exemple, la **perte** de **disponibilité**, de **confidentialité** et **d'intégrité**.»*

[ISO/CEI 27000 : 2012]

Objectifs de la Sécurité

- Les objectifs de la sécurité des systèmes d'information sont donc d'assurer la protection des actifs informationnels au regard de trois critères :
  - ✓ **Disponibilité**
  - ✓ **Intégrité**
  - ✓ **Confidentialité.**
- Ces trois critères sont fondamentaux et serviront également à qualifier et quantifier les risques sur le système d'information lors de l'Analyse de Risques.
- En outre, d'autres propriétés telles que **l'authenticité**, **l'imputabilité**, la **non-répudiation** peuvent également être recherchées.

Disponibilité

- « Propriété d'être accessible et utilisable à la demande par une entité autorisée.» [ISO/CEI 13335-1:2004]

- Aptitude d'un système informatique à pouvoir être employé à un instant donné par les utilisateurs.

- Disponibilité = la probabilité de pouvoir mener correctement à terme une session de travail

- L'indisponibilité est considérée comme une composante de la sécurité car peut entraîner des pertes financières.

Disponibilité

- La **disponibilité** est de pair avec son **accessibilité**
  - Une ressource doit être accessible, avec un temps de réponse acceptable.
- La disponibilité des services, systèmes et données est obtenue
  - par un dimensionnement approprié,
  - par une gestion opérationnelle des ressources et des services.
- Ce paramètre est mesuré par une montée en charge du système afin de s'assurer de la totale disponibilité du service
- Un service doit aussi être assuré avec le minimum d'interruption en respect avec l'engagement établi.
- De plus des pertes de données sont possibles si l'enregistrement et le stockage ne sont pas gérés correctement, d'où l'importance d'une **haute disponibilité** d'un système et de la mise en place d'une **politique de sauvegarde**.

Intégrité

- « Propriété de protection de l'exactitude et de l'exhaustivité des actifs. » Selon [ISO/CEI 13335-1 : 2004]

- L'intégrité permet de certifier que les données, les traitements ou les services n'ont pas été **modifiés**, **altérés** ou **détruits** tant de façon intentionnelle qu'accidentelle.

- L'altération est principalement occasionnée par le média de transmission mais peut provenir du système d'informations

- Il faut également veiller à garantir la protection des données d'une écoutes actives sur le réseau

Confidentialité

- « Propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés. » Selon [ISO/CEI 13335-1 : 2004]

- Dans le cadre d'un système d'information, la confidentialité peut être vu comme une protection des données contre une divulgation non autorisée
- Deux actions complémentaires permettant d'assurer la confidentialité des données
  - Limiter leur accès par un mécanisme de contrôle d'accès
  - Transformer les données par des procédures de chiffrement
- Classification des données selon la confidentialité :

  publique → privée → secrète → Top secrète

Identification - Authentification

- L'identification de l'auteur d'un document peut être aisé par contre être en mesure d'assurer l'authenticité du document est chose plus délicate
- Ces mesures doivent être mises en place afin d'assurer
  - La confidentialité et l'intégrité des données d'une personne
  - La non répudiation, c'est à dire qu'une personne identifiée et authentifiée ne peut nier une action
- L'identification peut être vu comme un simple nom d'utilisateur de connexion sur un système.
- L'authentification peut être un mot de passe connu seulement par l'utilisateur.
- Identification = se faire connaitre du système (avoir une identité)
- Authentification = prouver qui en est (avoir une preuve sur l'identité).

Non-répudiation

- La **non-répudiation** est le fait de ne pouvoir nier ou rejeter qu'un événement a eu lieu
- A cette notion sont associées
  - L'**imputabilité** : une action a eu lieu et automatiquement un enregistrement, preuve de l'action, est effectué.
    L'imputabilité se définit par l'attribution d'une action (un événement) à une entité déterminée (ressource, personne).
    L'imputabilité est liée à la notion de responsabilité. Elle peut être réalisée par un ensemble de mesures garantissant l'enregistrement fiable d'informations pertinentes par rapport à une entité et à un événement.
  - La **traçabilité** : mémorisation de l'origine du message
  - L'**auditabilité** : capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement.
- L'existence de fichiers journal (log) permet de garantir l'imputation et l'auditabilité

Principes de Mise en Œuvre de la Sécurité

P1. Disponibilité – Intégrité – Confidentialité :

- Le respect de ces propriétés est un principe de base et la mise en œuvre de mesures de sécurité doit s'attacher en priorité à s'en assurer.
- Les moyens à utiliser pour y parvenir seront déterminés à la fois par la **classification** des actifs informationnels au regard de ces critères et par l'**analyse des risques** auxquels ils sont exposés.

P2. Besoin d'en Connaître

- Les utilisateurs ne devraient avoir accès qu'aux informations ou aux systèmes strictement nécessaires à l'exécution de leur mission.
- Ce principe est utilisé essentiellement en environnement militaire ou gouvernemental, mais il peut aussi trouver des applications dans le monde civil, notamment bancaire, afin d'éviter le délit d'initié.

Principes de Mise en Œuvre de la Sécurité

P3. Moindre privilège

- Les utilisateurs devraient bénéficier uniquement du niveau d'accès minimal leur permettant d'accomplir leurs tâches.
- **Remarque:** Ce principe est également connu sous le nom de **Séparation des Privilèges** et est mis en pratique par exemple sous Windows 7 en distinguant les activités "Administrateur" des autres activités courantes d'un utilisateur.

P4. Séparation des Pouvoirs

- Le principe de séparation a la même finalité en sécurité informatique que dans la vie courante :

➢ Nul ne devrait être en mesure ou responsable d'accomplir, seul et de bout en bout, une tâche mettant en jeu une information sensible, critique ou de grande valeur.

➢ Nul ne devrait être responsable de l'approbation ou de la validation de son propre travail.

Principes de Mise en Œuvre de la Sécurité

P5. Interdiction par défaut

- Tout ce qui n'est pas explicitement autorisé, est « implicitement » interdit.

D'autres principes peuvent être considérés :

- **Défense en profondeur**
  Protection au plus tôt et à tous les niveaux
- **Goulet d'étranglement**
  Point de sortie unique permettant le contrôle
- **Concertation**
  Accepter les contraintes par les utilisateurs
- **Simplicité**
  Filtrage le plus simple possible
- **Maillon faible**
  Répartir équitablement les moyens de sécurité

Les Mesures ou Contrôles de Sécurité

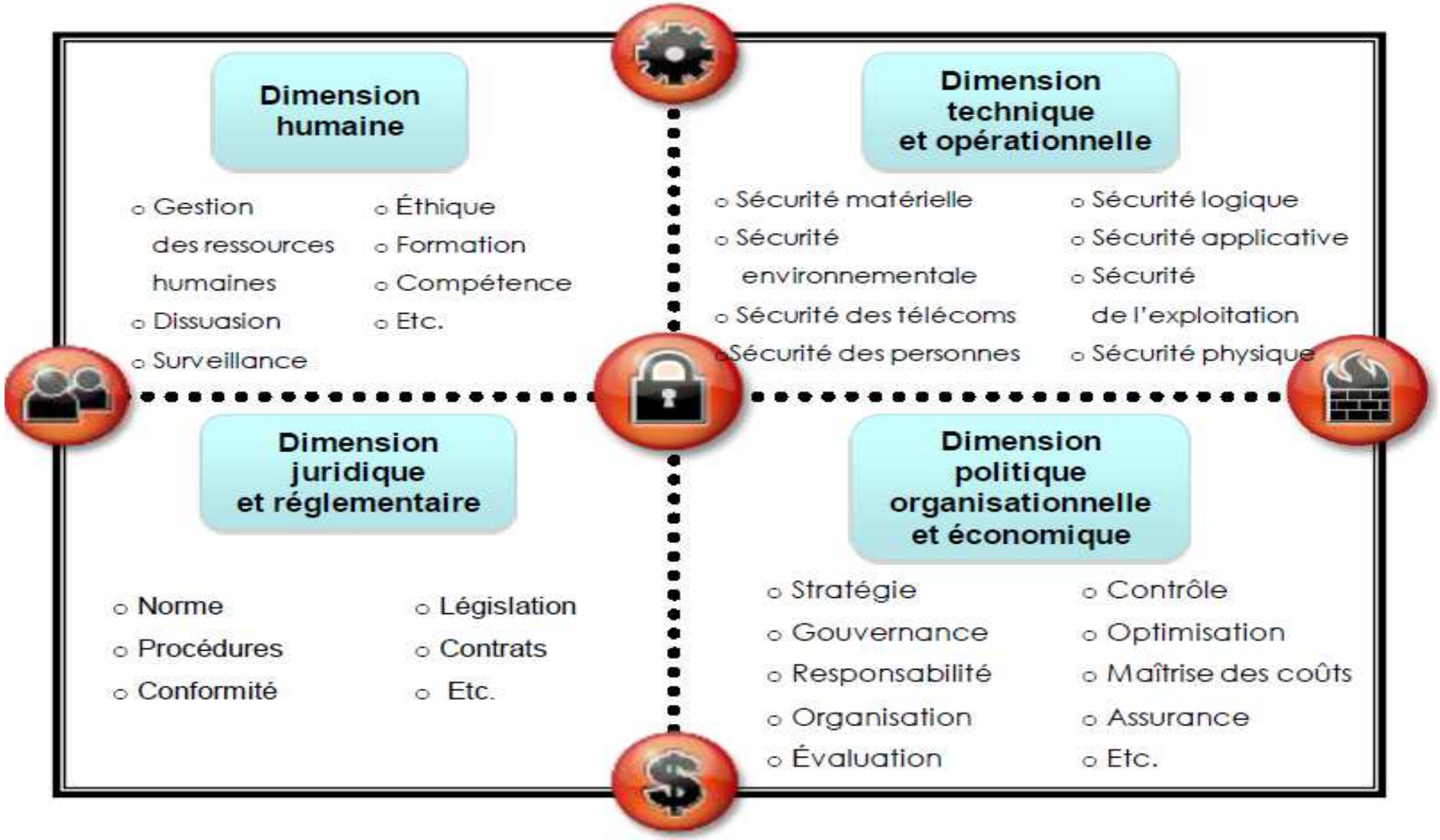
- Les contrôles de sécurité représentent les moyens organisationnels, opérationnels et techniques mis en œuvre au sein d'un système d'information afin d'en protéger la disponibilité, l'intégrité et la confidentialité :

- **Moyens Organisationnels :** Politique de sécurité > normes, processus > procédures > lignes directrices.

- **Moyens Opérationnels :** Sécurité physique, protection des infrastructures, plan de secours, procédures de maintenance, gestion de configuration, gestion des incidents, formation

- **Moyens Techniques :** Identification et authentification, contrôle d'accès logique et physique, audit, protection des systèmes et des communications, cryptographie

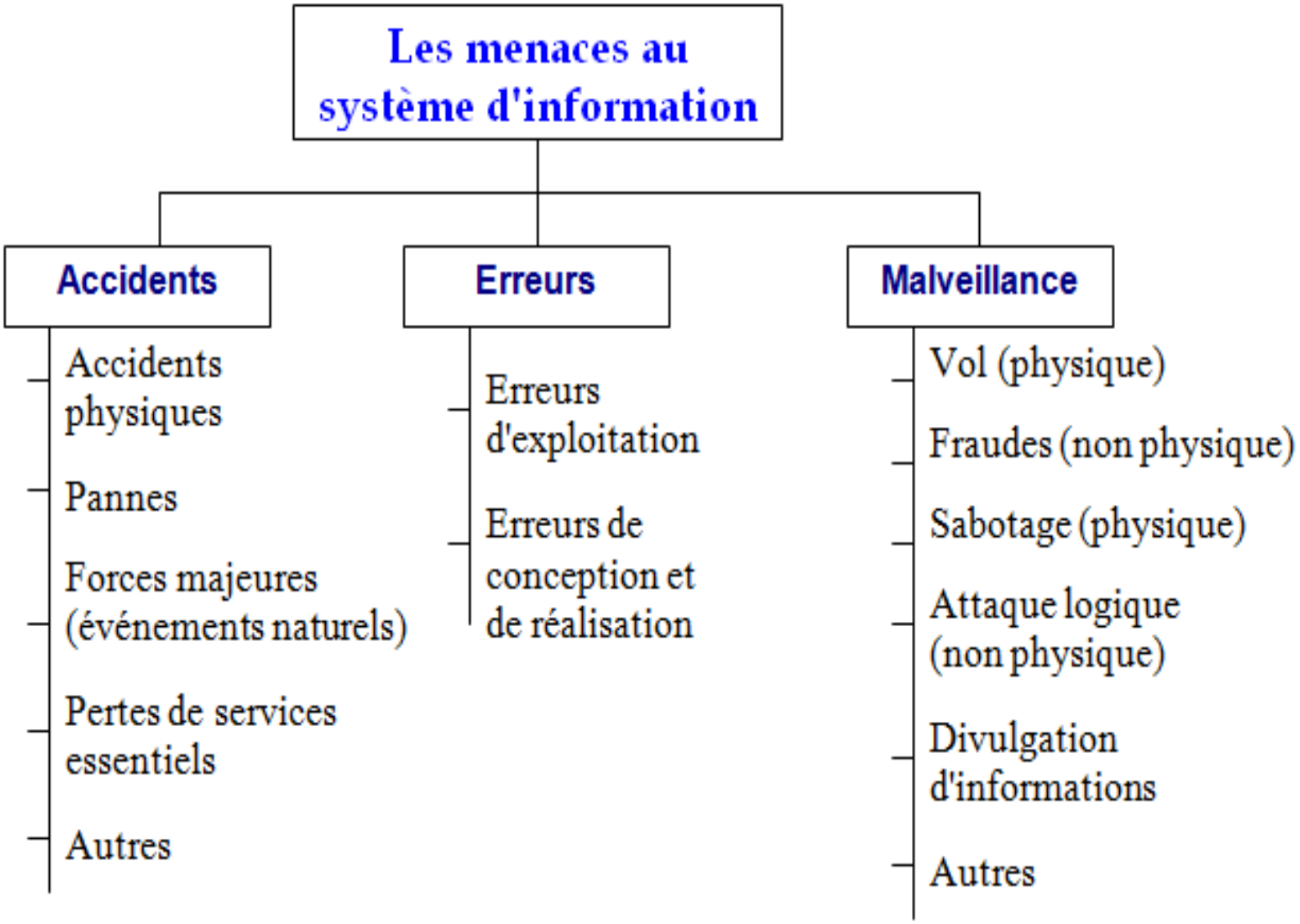
Architecture de sécurité



Architecture de sécurité

- Cette architecture est indispensable si l'on veut prendre en compte l'ensemble des problèmes de sécurité d'une entreprise
- Elle permet d'identifier les critères minima de sécurité pour chacun des éléments
- Permet également d'harmoniser le niveau de sécurité dans toutes les dimensions

Sources du problème



Deux dangers majeurs guettent les SI :

1. Perte de données

Les causes courantes sont :

- la "volonté de dieu" (?) : Feu, inondations, tremblements de terre, guerres, émeutes, rats, ….
- les erreurs matérielles ou logicielles : Fonctionnement défectueux du processeur, disques et bandes illisibles, erreurs de télécommunication, bogues dans les programmes, …
- les erreurs humaines : Saisie de données erronées, utilisation d'un mauvais disque, mauvaise exécution d'un programme, perte d'une disquette,…

➔ La solution universelle à ces problèmes : la **sauvegarde**

2. Fuite de données et intrusions

Les causes courantes sont :

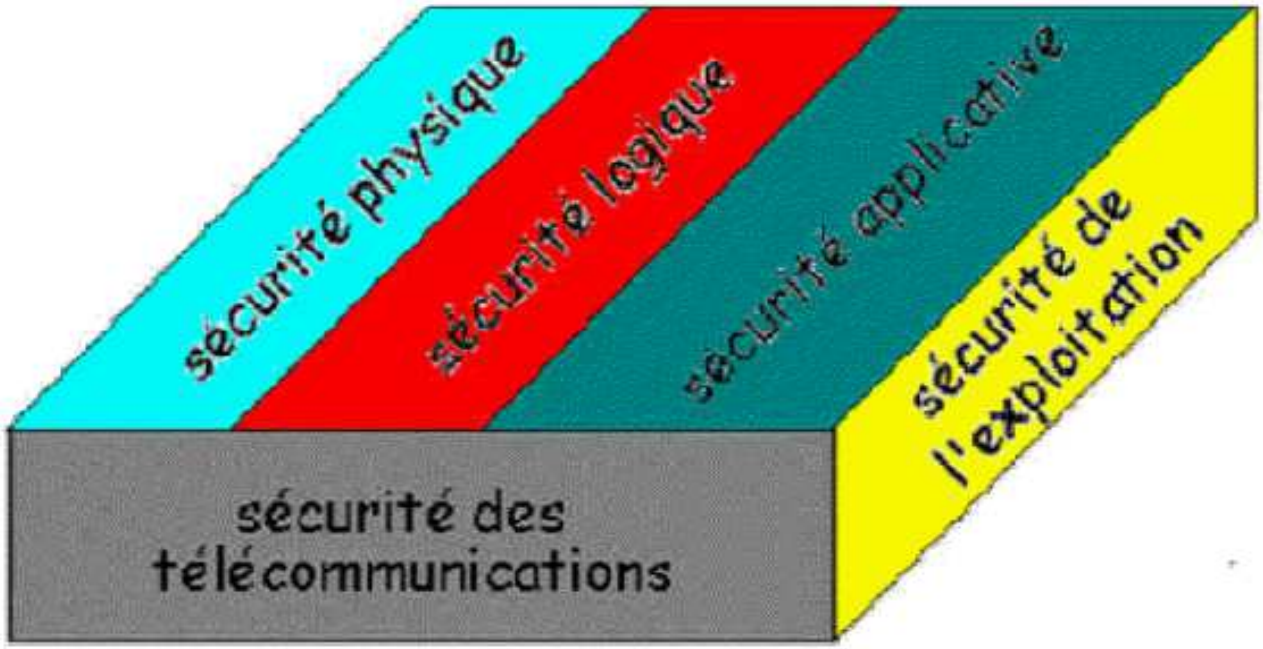
- Indiscrétion des utilisateurs
- Furetage
- Appât du gain : modification de données, vente d'information, chantage informatique
- Espionnage industriel ou militaire

➔ Les solutions sont les **mécanismes de protection** :

- Identification, Authentification, Autorisation
- Cryptographie
- Firewalls
- Audit
- Logiciels anti-virus
- Programmes de tests de vulnérabilité et d'erreurs de configuration
- Détection d'intrusion

Les aspects de la sécurité informatique

- Les objectifs de la sécurité informatique sont :
  - Réduire les risques technologiques
  - Réduire les risques informationnels dans l'utilisation des SI
- Il existe plusieurs domaines de sécurité :



Domaines de la sécurité informatique

1. Sécurité Physique

- liée à tous les aspects liés à la maitrise des systèmes et de l ’environnement dans lequel ils se situent.
- La sécurité repose essentiellement sur :
  - les normes de sécurité;
  - la protection des sources énergétiques (alimentation, etc.);
  - la protection de l’environnement (incendie, température, humidité, etc.);
  - la protection des accès (protection physique de équipement, locaux de répartition, tableaux de connexion, infrastructure câblée, etc.);
  - la sureté de fonctionnement et la fiabilité des matériels (composants, câbles, etc.);
  - la redondance physique;
  - le marquage des matériels;
  - le plan de maintenance préventive (test, etc.) et corrective (pièce de rechange, etc.);
  - - …

Domaines de la sécurité informatique

2. Sécurité logique

- Mécanismes logiciels de sécurité,
  - Contrôle d'accès logique : identification, authentification, autorisation
  - Protection des données : cryptage, anti-virus, sauvegarde

- La sécurité logique fait référence à l' élaboration de solutions de sécurité par des logiciels contribuant au bon fonctionnement des applications et services.

- La sécurité logique repose en grande partie sur des techniques de cryptographie par des procédures d'authentification, par des antivirus, des procédures de sauvegarde et de restitution des informations sensibles sur des supports fiables et spécialement protégés et conservés dans des lieux sécurisés.

- Afin de déterminer le degré de protection nécessaire aux informations manipulées, une **classification des données** est à réaliser afin de qualifier leur degré de sensibilité (normale, confidentielle, etc.).

Domaines de la sécurité informatique

3. Sécurité applicative

- l'objectif est d'éviter les « **bugs** » :
- La sécurité applicative comprend le développement de solutions logicielles (ingénierie du logiciel, qualité du logiciel) ainsi que leur intégration et exécution harmonieuses dans des environnements opérationnels.
- Elle s'appuie essentiellement sur l'ensemble des facteurs suivants:
  - une méthodologie de développement (respect des normes);
  - la robustesse des applications;
  - des contrôles programmés;
  - des jeux des tests;
  - des procédures de recettes;
  - l' intégration de mécanisme de sécurité, d'outils d' administration et de contrôle de qualité dans les applications;
  - un plan de migration des application critiques;
  - la validation et l'audit des programmes;
  - un plan d'assurance sécurité;
  - …

Domaines de la sécurité informatique

4. Sécurité de l'exploitation

- concerne tout ce qui est lié au bon fonctionnement des systèmes informatiques.
- La sécurité de l'exploitation dépend fortement de son niveau d'industrialisation, qui est qualifié par son niveau de supervision des applications et l'automatisation des tâches.
- Les points critiques de la sécurité de l'exploitation sont les suivant :
  - plan de sauvegarde;
  - plan de secours;
  - plan de continuité;
  - plan de tests;
  - inventaires réguliers et si possible dynamique;
  - gestion du parc informatique;
  - gestion des configuration et des mises à jour;
  - gestion des incidents et suivi jusqu' à leur résolution;
  - analyse de fichiers de journalisation et de comptabilité;
  - …

Domaines de la sécurité informatique

5. Sécurité de télécommunication

- consiste à offrir à l'utilisateur final une connectivité fiable et de qualité de bout en bout (end to end security).
- Ceci implique l'élaboration d'une infrastructure réseau sécurisée au niveau
  - des accès,
  - de l'acheminement ,
  - des protocoles de communication,
  - des systèmes d'exploitation,
  - des équipements de télécommunications,
  - des supports de transmission.
- La sécurité des télécommunications ne peut à elle seule garantir la sécurité des transfert des données. Il est également impératif de sécuriser l'infrastructure applicative dans laquelle s'exécutent les applications sur les systèmes d'extrémité au niveau de l'environnement de travail de l'utilisateur et des applications.
- Le sécurité des télécommunications ne peut s'envisager sans une analyse de risque spécifique à chaque organisation en fonction de son infrastructure *environnementale*, *humaine*, *organisationnelle* et *informatique*.

Domaines de la sécurité informatique

- Quatre problèmes principaux à résoudre