Partie I:

- I.1 De la sécurité des biens et personnes à la sécurité informatique
- I.2 Enjeux de la sécurité Informatique
- **I.3 Propriétés / Services de la sécurité**
- I.4 Vulnérabilités, Failles, Menaces, Attaques

Les Besoins de Sécurité

- **Question**: Comment définir le niveau/besoin de sécurité d'un bien d'un SI?

➔ bien: c'est ce qu'on désire protéger (donnée, répertoire, serveur, imprimante, accès réseau, BDD, etc.)

❑ Exemple: Par rapport à vos emails, qu'est ce qui est le plus important:

- Accessible quand vous le voulez (à n'importe quel moment)
- Ne sont lisible que par vous uniquement
- S'assurer que ce que vous recevez comme mails est vraiment les emails que contient votre boite sur le serveur
- S'assurer que la personne ayant envoyé un mail est la personne qu'elle prétend être
- ....

Les Besoins de Sécurité

Question: Comment s'assurer/évaluer que ce bien est correctement protégé/sécurisé?

- Comment s'assurer que vos emails sont accessible uniquement à vous et qu'il n'y a pas une autre personne qui y a accès?
- Comment s'assurer qu'un mail reçu a été vraiment envoyé depuis la boite email de la bonne personne? (expéditeur)
- Comment s'assurer que mon serveur email est toujours accessible

Les Besoins en Sécurité

- Pour répondre à ces questions, des **critères** ont été adoptés, et ceci pour répondre aux **besoins** en termes de sécurité d'un bien SI, mais aussi pour s'assurer et **évaluer** si le bien est bien protéger

- 3 Critères/Services fondamentaux de de Sécurité, **DIC**(P):

- **D**isponibilité
- **I**ntégrité
- **C**onfidentialité
- **(P**reuve)

Les Besoins en Sécurité

- **Disponibilité** (Availability)

- C’est la propriété qu’un bien soit disponible/accessible au moment voulu (durant plages temporel/spatiale prévus)

- **Disponibilité** du réseau de téléphonie mobile, sur tout le territoire national -ou au moins sur toute la couverture annoncée par l’opérateur- 7/7J; 24/24H

- **Disponibilité** des serveurs google, facebook, yahoo, etc.

- **Disponibilité** des distributeurs automatique d’argents et des terminaux de paiements

- **Disonibilité** d’accès à Internet pour les institution financières, et les e-commerçants

Les Besoins en Sécurité

- **Intégrité (Integrity)**

- C’est la propriété d'exactitude d’un bien où d’une information, qui garantit que ce bien n’a pas été **altéré/modifié** d’une façon illicite, et si c’est le cas, ceci sera détecté, voir même corrigé
- L’Université voudrait bien s’assurer que les notes de étudiants telles qu’elles ont été remis par le prof et saisis sur le BDD, n’ont pas été modifiées
- Lors d’un achat en ligne, si je passes un commande d’une valeur de **200 $**:

➢ Moi et ma banque on voudrait bien s’assurer que c’est exactement **200$** - non pas **250$**- qui sera débité de mon compte

➢ Le vendeur et sa banque voudrait bien s’assurer que c’est la somme de **200$** - non pas **150 $** - qui sera crédité sur son compte

Les Besoins en Sécurité

- **Confidentialité** (Confidentiality)

- C’est la propriété qu’une donnée soit **accessible** uniquement à la (les) **personne**(s) **autorisé**(s) → Le reste, est supposée normalement inerdit d’accès d’une quelconque façon.

- Chaînes cryptés, accessible uniquement aux détenteurs de carte

- Sur un PC où il y a plusieurs comptes utilisateurs, chaque utilisateur a uniquement l'accès à ses données et non pas aux données des autres utilisateurs (sauf admin)

- Les mots de passe qu’on utilise (FB TW, mails, etc.), sont confidentiel

- Les informations compte bancaire/postale sont supposé être confidentiel

Les Besoins en Sécurité

- **Peuve** où **Traçabilité**

- Ce critère/Service n'étant pas fondamentale, mais est souvent associé aux critères **DIC**. Il représente la propriété de pouvoir **retrouver** les **circonstances** dans lequel un bien **évolue**. Cette propriété englobe le plus souvent:

➔ La **traçabilité** des actions menés (ex, fichier log)

➔ L'**authentification** des utilisateurs (ex, login/mot de passe)

➔ L'imputabilité de responsable de l'action effectué (une personne qui s'est connecté à un site interdit depuis son lieu de travail)

Exemple: Lors d'une transaction e-commerce , la propriété Preuve, permettra de prouver que le compte client à été débiter, et celui du vendeur a été créditer.

Anologie avec le monde réel :

- Lors d'un délit/crime, les enquêteurs doivent pouvoir présenter des preuves (prouver) la culpabilité de l'auteur présumé (empreintes, ADN, vidéos, ...)
- A/R d'une lettre, preuve de la réception de la lettre

Les Besoins en Sécurité

- **Évaluation DICP**

- **Q**: Comment s'assurer qu'un bien est bien sécurisé/protégé?

- **R**: Il Faut **auditer/évaluer** son niveau de **D**, **I**, **C** et **P** sur une échelle

---------- **Par analogie** ----------

- **Q**: Comment s'assurer qu'une voiture est conforme aux normes de mise en circulation en DZ (Test Freinage, Test impact, Test de stabilité, seuil pollution, consommation etc.)

- **R**: Il faut auditer (faire une expertise) de ses performances par rapport aux différents critères relevant de la norme de mise en circulation sur une échelle, et puis affecter une note à chaque critère passé

Les Besoin en Sécurité

- **Évaluation DICP**

- **Q**: Pourquoi avons nous besoin d'une échelle pour l'évaluation?
- **R**: Car les biens d'un SI d'une entreprise n'ont pas besoin d'atteindre le même degrés de besoin de protection (niveaux DICP)
- Pour certaines biens la Confidentialité est plus importante, donc les autres besoins passent au 2ème plan
- Pour d'autres biens, la Disponibilité est primordiale, pour d'autres c'est l'intégrité, pour 'autres c'est la traçabilité
- Pour d'autres tous les besoins d'avoir avoir le niveau max
- **Par anologie**: le degrès de sécurité des maires, chef daire, walis, ministres, premier ministre, et président n'est pas le même! Ça se voit en matière de moyens déployés pour assurer leur sécurité

Les Besoin en Sécurité

- **Évaluation DICP**

- Exemple: Au sein d'une même base de données, certains données (champs, attributs) ont besoin d'un niveun de confidentialité plus élevé que d'autres

- Exemple; Les codes de lancement/désactivation nucléaires USA des têtes nucléaires, leur emplacement, le noms des agnts CIA à l'étranger, les opérations clandestines non légales (kidnapping, assassinats, espionage, etc.) sont toutes des informations secrets mais n'ayant pas le même degrés de confidentialité et d'accès

Le Besoin en Sécurité

- **Évaluation DICP**

- Suite à une évaluation d'un bien (ex, serveur Web), nous avons obtenu les résultat suivant sur une échelle (Très Fort, Fort, Moyen, Faible)

Niveau de Disponibilité du bien	Très fort
Niveau d'Intégrité du bien	Moyen
Niveau de Confidentialité du bien	Très fort
Niveau de Preuve du bien	Faible

Le bien bénéficie d'un niveau de sécurité adéquat

Les Besoin en Sécurité

- **Évaluation DICP**

- Exemple: un site d'une entreprise (statique) qui vise à faire de la publicité pour l'entreprise

Disponibilité = Très fort

Un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaitre ses services au public

Intégrité = Très fort

Un haut niveau d'intégrité des informations présentées est nécessaire. En effet, l'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site web pour y insérer des informations erronées (ce qui serait dommageable)

Serveur web

Confidentialité = Faible

Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature!

Preuve = Faible

Un faible niveau de preuve suffit. En effet, ce site web ne permet aucune interaction avec les utilisateurs, il fournit simplement des informations fixes.

Les Besoins en sécurité

- Les besoins en sécurité (niveaux DCIP) de certains biens à protéger peuvent varier dans le temps
- Exemple: Lors d'une soumission en ligne à un appel d'offre, les données doivent **rester confidentiel** jusqu'à l'instant **J** d'ouverture des plis électroniques, audelà ils peuvent être digulgués.

- Un sujet d'examen électronique doit rester confidentiel jusqu'à l'instant où il est supposé se dérouler

- **Par anologie**: le degrès de sécurité d'un président en exercice n'est pas le même quand ce dernier quite le poste!

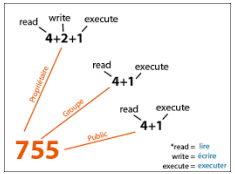
Les Besoins en sécurité: Mise en oeuvre

- En pratique Comment mettre en oeuvre les Besoins en Sécurité (concrètement comment fournir ces services de sécurité)?

-Une panoplie de mécanismes, méthodes, pratiques, Software/Hardware, etc.

Antivirus 	• Un Logiciel faisant fasse à un ou plusieurs logiciels malveillants(virus, malware, spamware, rançomware, etc.) étant à priori détecté comme tels - Kaspersky, Symantec, Avast, etc.
Cryptographie 	• Mécanisme permettant d'implémenter (SW/HW, mixte) -en partie- les services ICP - AES, RSA, etc.
Pare-Feu 	• Mécanisme -HW le plus souvent, mais aussi SW- permettant de filtrer le traffic depuis/vers une machine où un réseau - Par-Feu Windows, iptables (unix), Cisco,

Les Besoins en sécurité: Mise en oeuvre

Contrôle accès Logique  	● Mécanismes permettant de restreindre l'accès aux ressources informatiques (données, fichiers, répertoires, serveurs, machines, etc.) ● Accès: Lecture, Écriture, Modification, Destruction, Copie, etc. - Login (Ouverture Session), Gestion droits/utilisateurs unix, etc.
Sécurité Physique Locaux Équipements 	● Mécanismes de protection destiné à protéger l'intégrité physique du matériel et des bâtiments/locaux - Locaux hébergeant les serveurs/BDD fermés à clés avec accès contrôlé. - Serveurs, machines scellés - Poste de sécurité, caméras de surveillance, clôture, etc.

Les Besoins en sécurité: Mise en oeuvre

Formation Sensibilisation  	● Mécanismes organisationnels visant à la: - Formation continue du personnel dédié à la sécurité Informatique, aux nouvelles menaces, et les nouvelles technologies de contre-mesures ● Formation, sensibilisation des autres employés aux risques et aux bonnes pratiques à adopter
Audits 	● Mécanismes organisationnels visant à s'assurer de l'efficacité et de la pertinence des mesures de sécurité mises en place ● Suite à une audit, des recommandation peuvent être formulés, indiquant certaines faiblesse/lacunes, participant ainsi à l'amélioration en continue de la sécurité du SI

Les Besoins en sécurité: Mise en oeuvre

- ***Définition de la sécurité Informatique**:*

L’ ensemble des **moyens** et **mécanismes (techniques et non techniques)** mis en place, destinés à **protéger** l'information, les systèmes d’informations et les services, des utilisateurs ou processus n'ayant pas l'autorisation de les accéder et/ou manipuler.

La sécurité informatique à pour objectif de fournir et garantir les services de DCIP