Sécurité Informatique

Chapitre I : Introduction à la Sécurité Informatique

Bourbia.riad@univ-guelma.dz

Plan du cours

1. Définitions
2. Principaux concepts de sécurité informatique
3. Objectifs de la SI
4. Les menaces et leurs Impacts
5. Nécessité d'une approche globale
6. Mise en place d'une politique de sécurité

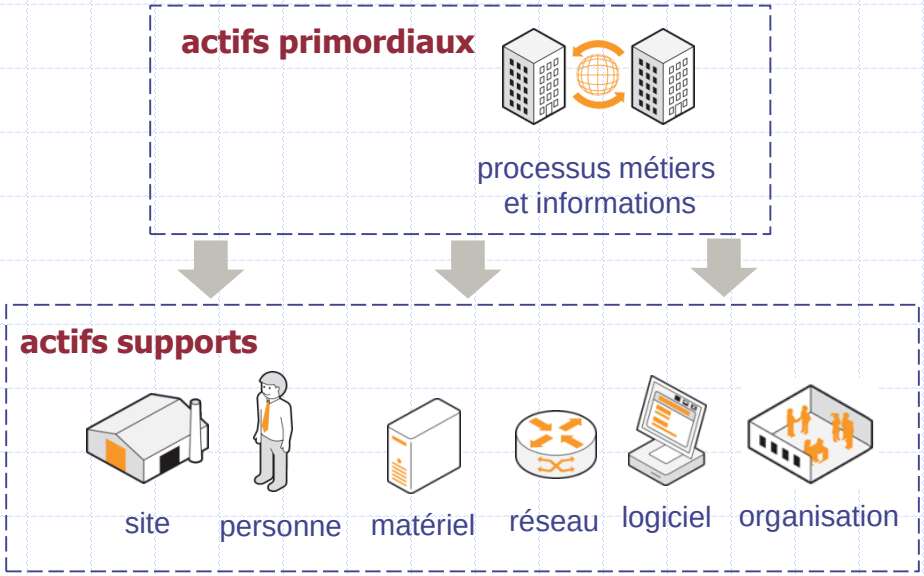

AUJOURD'HUI LES BANDITS NE SONT PLUS SUR LES GRANDS CHEMINS...
ILS SONT SUR LES AUTOROUTES DE L'INFO !
FAUJOUR

1. Définitions

Systèmes d'information (SI)

- Ensemble des ressources destinées à collecter, classifier, stocker, gérer, diffuser les informations au sein d'une organisation
- Mot clé : information, c'est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.

- Le système d'information d'une organisation contient un ensemble d'actifs :



1. Définitions

Sécurité des SI

La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens

État de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour assurer la confidentialité, l'intégrité et la disponibilité du système et de l'information traitée.

Différences entre sureté et sécurité

« Sûreté » et « Sécurité » ont des significations différentes en fonction du contexte. L'interprétation de ces expressions peuvent varier en fonction de la sensibilité de chacun.

Sûreté

Protection contre les dysfonctionnements et accidents involontaires

Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.

Quantifiable statistiquement (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)

Parades : sauvegarde, dimensionnement, redondance des équipements…

Sécurité

Protection contre les actions malveillantes volontaires

Exemple de risque : blocage d'un service, modification d'informations, vol d'information

Non quantifiable statistiquement, mais il est possible d'évaluer en amont le niveau du risque et les impacts

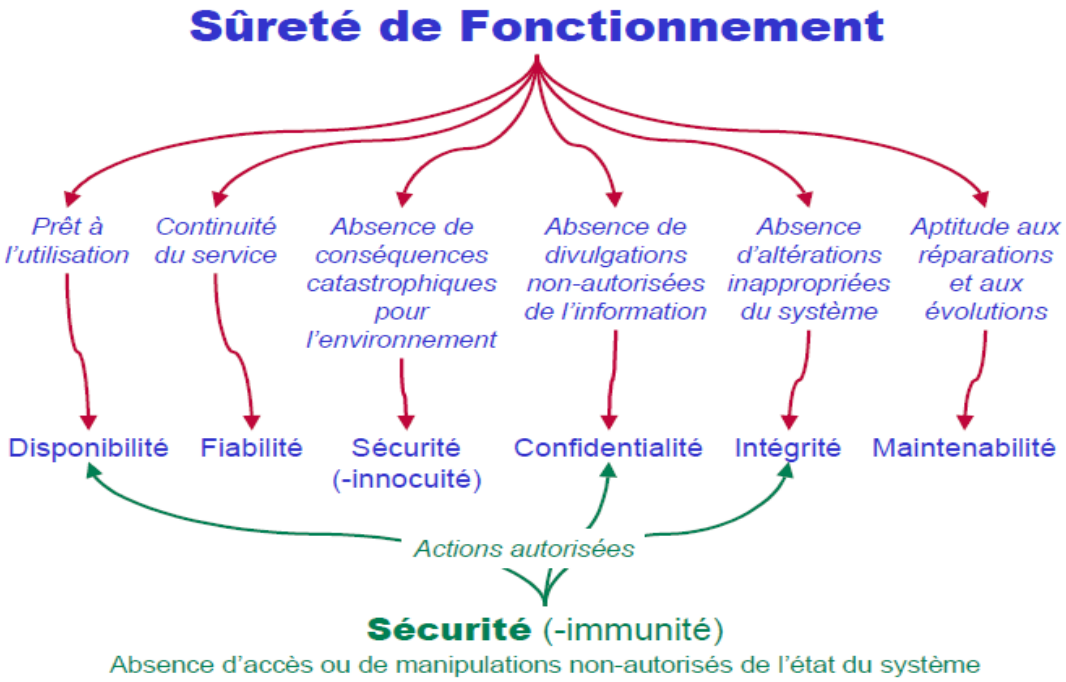
Parades : contrôle d'accès, veille sécurité, correctifs, configuration renforcée, filtrage…*

Différences entre sureté et sécurité

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.

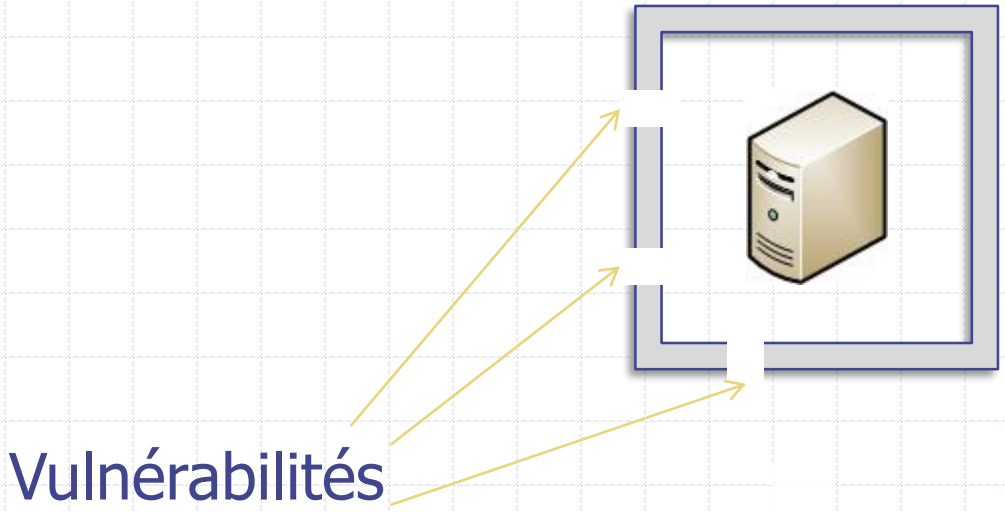
Le périmètre de chacune des 2 notions n'est pas si clairement délimité dans la réalité : dans le cas de la voiture connectée on cherchera la sécurité et la sûreté.



2. Principaux concepts de sécurité informatique

Notion de « Vulnérabilité »

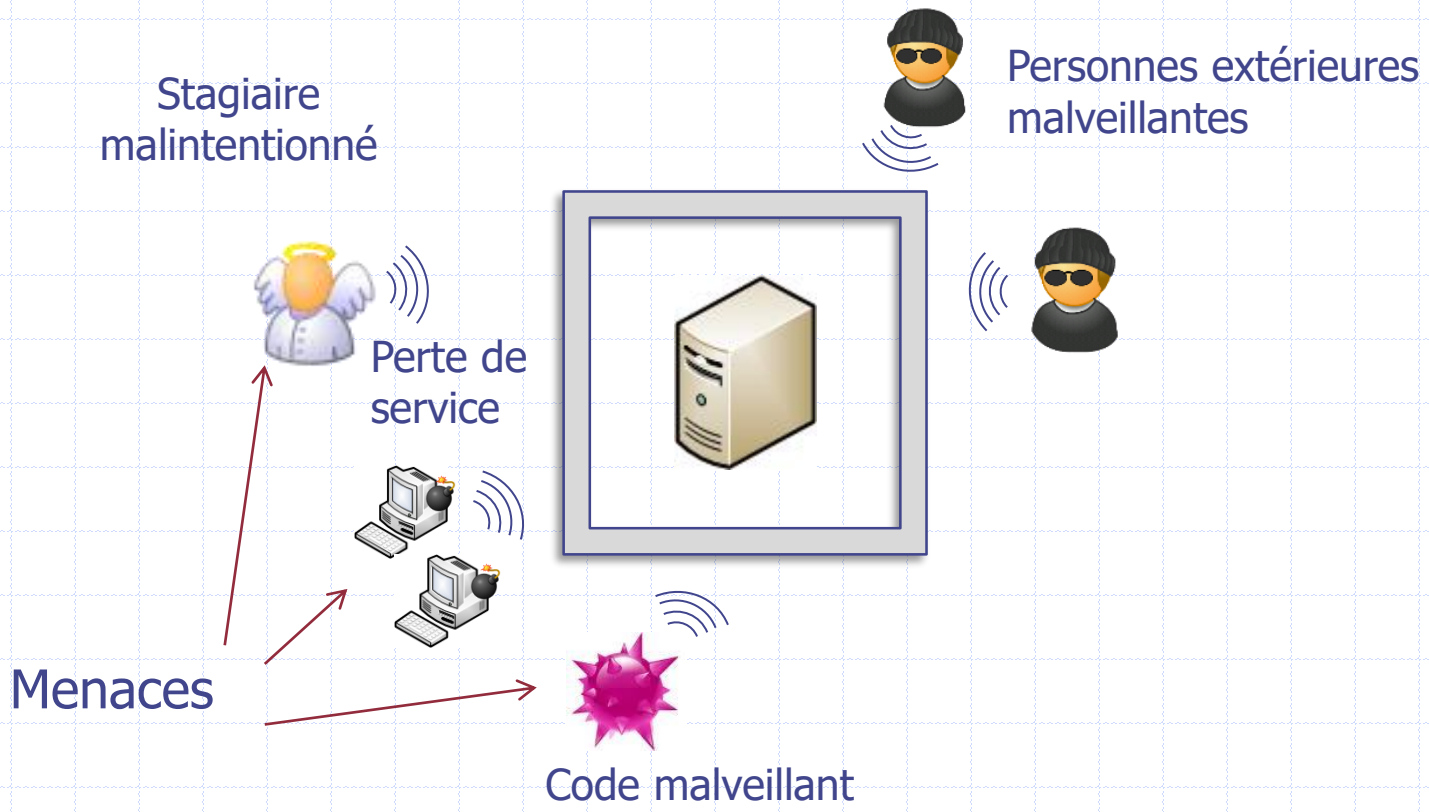
- **Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



2. Principaux concepts de sécurité informatique

Notion de « Menace »

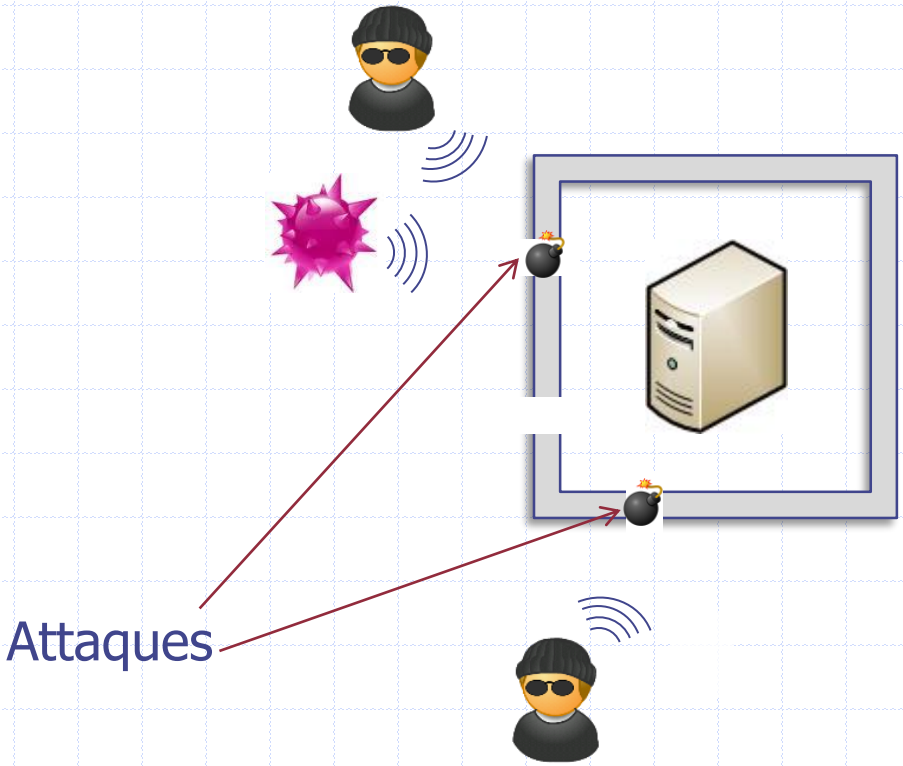
- **Cause *potentielle* d'un incident**, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



2. Principaux concepts de sécurité informatique

Notion d'« Attaque »

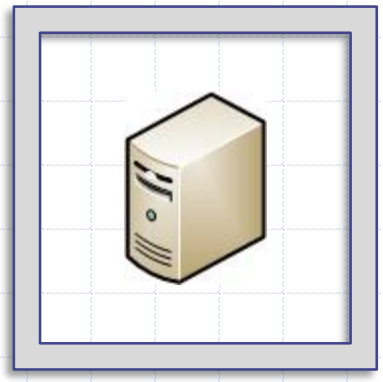
- **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité.**



2. Principaux concepts de sécurité informatique

Notion d'« Attaque »

- Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.



Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité.

Dans la réalité, l'objectif est en fait d'être en mesure de maitriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

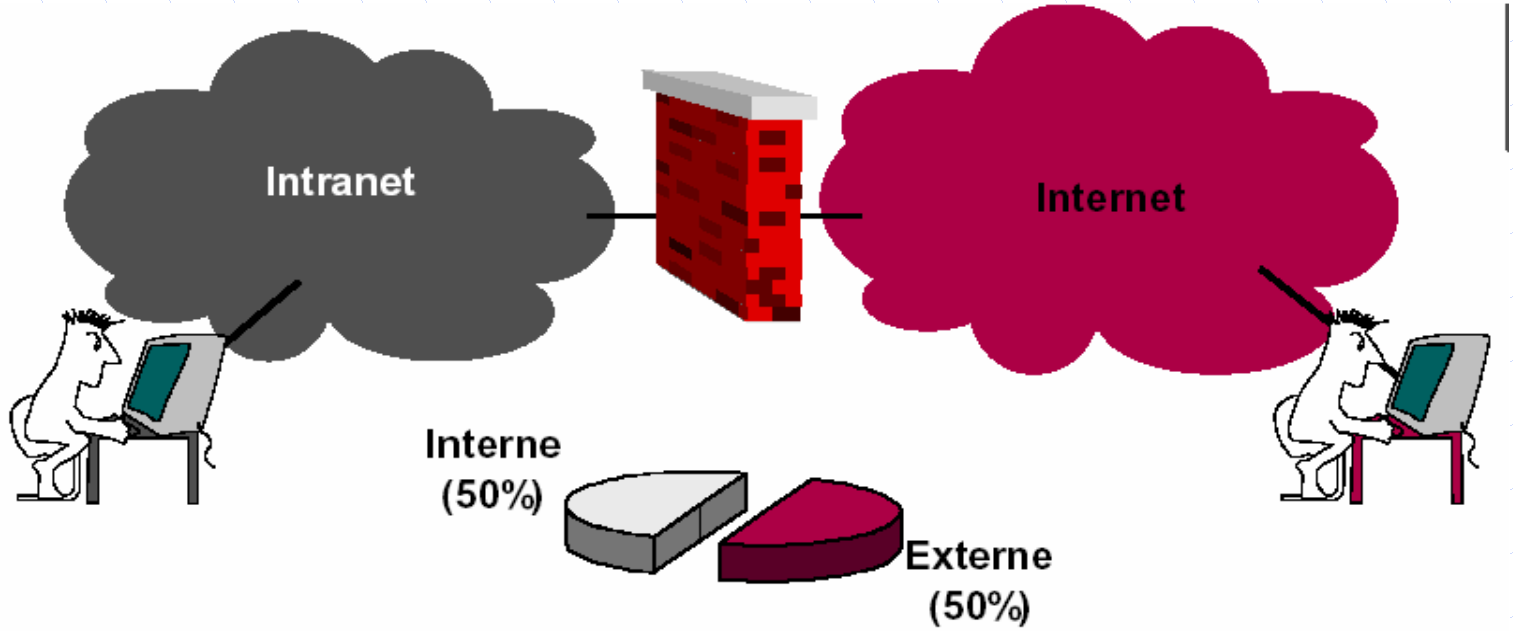
2. Principaux concepts de sécurité informatique

La contre-mesure est l'ensemble des actions mises en oeuvre en prévention de la menace.

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

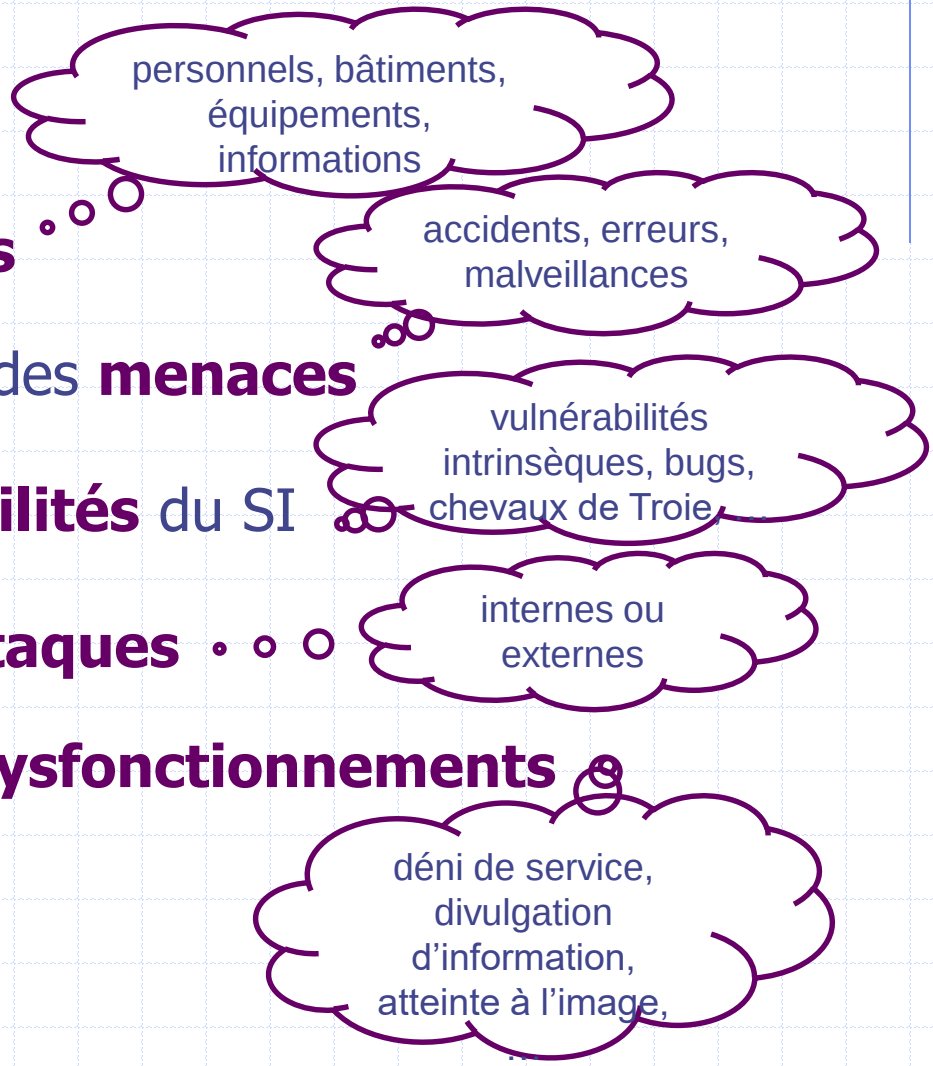
2. Principaux concepts de sécurité informatique

Origine des attaques



2. Principaux concepts de sécurité informatique

- Un SI gère des **biens**
- Qui sont sensibles à des **menaces**
- Liées à des **vulnérabilités** du SI
- Exploitées par des **attaques**
- Qui provoquent des **dysfonctionnements**



2. Principaux concepts de sécurité informatique

- Dont on évalue la **probabilité** et **l'impact**
- Afin d'estimer le **risque**

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

- Ce qui permet de choisir les **mesures** adaptées (techniques et non techniques)

Assurance conformité
Assurance efficacité

Introduction à la sécurité (Résumé)

[Autrement dit, Prendre en compte la sécurité des systèmes d'information c'est :]

- Garantir les **services** à rendre (paye, gestion des notes, comptabilité, GRH, …)
- par la mise en œuvre de **moyens techniques**
- Et par la définition d'une **organisation**

dans le but

- D'éviter les risques
- De détecter les attaques
- De limiter les dégâts

Introduction à la sécurité (Résumé)

- Eviter les risques
  - sensibiliser : développer la prise de conscience et l'implication
  - prévenir : empêcher l'occurrence de l'événement
  - dissuader : prévoir des sanctions
- Detecter les attaques
  - déceler et identifier l'agression
- De limiter les dégâts
  - confinement : empêcher la propagation
  - riposte : mettre en place des mesures de sauvegarde, de destruction de l'information, des actions contre l'agresseur
  - réparation : annuler les conséquences et recouvrer la situation antérieure.

Pour finalement augmenter la **confiance** du SI

3. Objectifs de la SSI

La sécurité informatique vise généralement cinq principaux objectifs :

- intégrité
- confidentialité
- disponibilité
- non-répudiation
- authentification

3. Objectifs de la SSI [Intégrité]

c'est-à-dire garantir que les données sont bien celles que l'on croit être ;

On ne peut modifier les informations stockées dans le système qu'à l´issue d'un acte légitime et volontaire [et/ou] on dispose d'un moyen sûr pour détecter une violation de l´intégrité;

Perte d'intégrité sans conséquence

Le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités de l'organisme

Ex : aucune vérification

3. Objectifs de la SSI [Intégrité]

Perte d'intégrité entraînant des gênes de fonctionnement

Susceptible de provoquer une diminution des capacités de l'organisme.

Ex : vérification des données, sans validation :des fautes d'orthographe sur une page web nuisent à l'image de marque du laboratoire

Perte d'intégrité entraînant des conséquences dommageables

Susceptible d'amoindrir les capacités de l'organisme, avec des conséquences telles que des pertes financières, sanctions administratives ou réorganisation

Ex : données qui sont validées et contrôlées par des moyens techniques ou humains

3. Objectifs de la SSI [Intégrité]

Perte d'intégrité entraînant des conséquences graves

Susceptible de provoquer une modification importante dans les structures et la capacité de l'organisme comme la révocation de dirigeants, la restructuration de l'organisme, des pertes financières.

Ex : données avec au moins deux niveaux de validation et de contrôle différents (techniques ou humains).

3. Objectifs de la SSI [confidentialité]

Consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées .

La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

Perte de confidentialité sans conséquence

Le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités de l'organisme

Ex : données publiques, visibles par tous.

3. Objectifs de la SSI [confidentialité]

- Perte d'intégrité entraînant des gênes de fonctionnement

Ex : données liées aux compétences ou savoir-faire internes, dans un contexte de groupe de confiance, dont vous protégez toutes les traces écrites.

- Perte d'intégrité entraînant des conséquences dommageables

Ex : données liées à un engagement de confidentialité dans un contrat.

- Perte d'intégrité entraînant des conséquences dommageables

Ex : données secret défense.

3. Objectifs de la SSI [disponibilité]

- **Permettant de maintenir le bon fonctionnement du système d'information ;**

L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources ;

Délai supérieur à une semaine

Des services qui apportent un confort supplémentaire mais pas indispensable.

3. Objectifs de la SSI [disponibilité]

Délai > 8 heures et <= 1 semaine

Ressources pour lesquelles il existe une alternative.

Ex : Imprimante.

Délai > 2heures et <= 8 heures

Sans conséquence vitale humainement

Ex : arrêt du réseau, de la messagerie, données vitales non disponibles...

Délai : entre temps réel et <= 2 heures

Ressources qui mettent en péril la vie (humaine ou animale ou biologique).

Ex : expériences biologiques ou physiques pilotées automatiquement,

3. Objectifs de la SSI

- La **non répudiation**, permettant de garantir qu'une transaction ne peut être niée

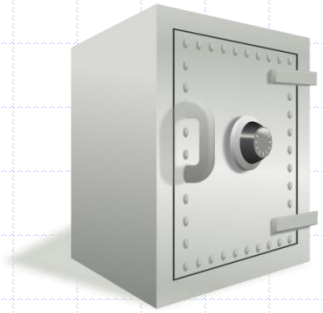
- L'**authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

L'authentification consiste à assurer l'identité d'un utilisateur. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

Les critères DIC

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?
- 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)

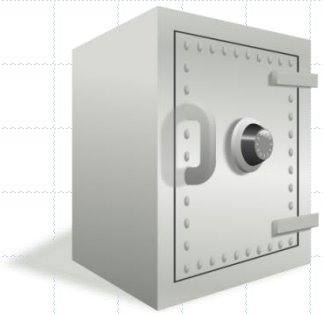
Intégrité — Propriété d'exactitude et de complétude des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)

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

Le critère Preuve

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?
- 1 critère complémentaire est souvent associé au D.I.C.

Bien à protéger



Preuve

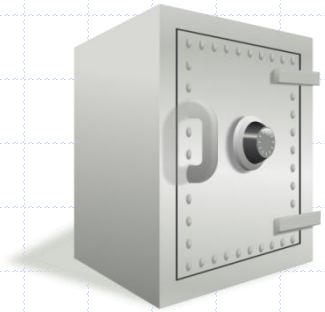
Propriété d'un bien permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe Notamment :

- La traçabilité des actions menées
- L'authentification des utilisateurs
- L'imputabilité du responsable de l'action effectuée

Exemple d'évaluation DICP

Ainsi, pour évaluer si un bien est correctement sécurisé, il faut auditer son niveau de Disponibilité, Intégrité, Confidentialité et de Preuve. L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.

Exemple des résultats d'un audit sur un bien sur une échelle (Faible, Moyen, Fort, Très fort) :



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

Exemple d'évaluation DICP

- Tous les biens d'un S.I. n'ont pas nécessairement besoin d'atteindre les mêmes niveaux de DICP.
- Exemple avec un site institutionnel simple (statique) d'une entreprise qui souhaite promouvoir ses services sur internet :

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

Confidentialité = **Faible**

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

Serveur web

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)

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.

Mécanismes de sécurité pour atteindre les besoins DICP

Un Système d'Information a besoin de mécanismes de sécurité qui ont pour objectif d'assurer de garantir les propriétés DICP sur les biens de ce S.I. Voici quelques exemples de mécanismes de sécurité participant à cette garantie :

		D	I	C	P
Anti-virus	Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité	✓	✓	✓	
Cryptographie	Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques		✓	✓	✓
Pare-feu	Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement	✓		✓	
Contrôles d'accès logiques	Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dument habilitées		✓	✓	✓
Sécurité physique des équipements et locaux	Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.	✓	✓	✓	

4. Les menaces et leurs Impacts

Les impacts des attaques sur les critères de sécurité peuvent se traduire ainsi :

Critères	Attaques	Impacts
Confidentialité	Divulgation, accès par des tiers non autorisés et détournement à des fins délictueuses, de données confidentielles (touchant des travaux confidentiels, des données scientifiques ou technologiques, des données personnelles telles que médicales ou financières), que ces données soient stockées ou échangées (messagerie)	Pertes du patrimoine scientifique ; pertes d'avance technologique et technique ; pertes financières ; contentieux juridique

4. Les menaces et leurs Impacts

Critères	Attaques	Impacts
Disponibilité -	**Vol de matériel**, **émission de malware** (virus, ver, …) **Sinistres**	Interruption de service ; paralysie ou désorganisation conduisant à l'incapacité opérationnelle de fonctionnement, de décision, de gestion, de sécurisation ; perte de données précieuses (scientifiques ou de gestion) par absence ou insuffisance de sauvegarde ; atteinte à la sécurité du personnel, des usagers ; perte d'image de marque

4. Les menaces et leurs Impacts

Critères	Attaques	Impacts
Intégrité	Modification accidentelle ou délibérée (défiguration de sites Web…), émission de malware (bombes logiques, chevaux de Troie, sniffeurs…), vol ou détournement de moyens informatiques à des fins délictueuses (compromission de serveurs…)	Résultats de fonction incomplets ou incorrects ; expérimentations non crédibles ; prises de décisions inadaptées ; appropriation frauduleuse de biens ; prise de contrôle d'un système physique ; perte du patrimoine scientifique ; perte d'image de marque ; atteinte à des libertés individuelles (cybersurveillance indue…)

5. Nécessité d'une approche globale

La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible.

Exemple : Une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

- Une démarche globale

Chacun est détenteur de la sécurité et doit se sentir « partie prenante »

5. Nécessité d'une approche globale

On doit prendre en compte les aspects suivants :

- La **sensibilisation** des utilisateurs aux problèmes de sécurité
- La **sécurité logique**, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.
- La **sécurité des télécommunications :** technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.
- La **sécurité physique**, soit la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc.

6. Mise en place d'une politique de sécurité

La politique de sécurité est l'ensemble des orientations suivies par une organisation en terme de sécurité.

Elle doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

A cet égard, il ne revient pas aux seuls administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers.
Le rôle de l'administrateur informatique est donc de s'assurer que les ressources informatiques et les droits d'accès à celles-ci sont en cohérence avec la politique de sécurité définie par l'organisation.

6. Mise en place d'une politique de sécurité

La mise en oeuvre d'une politique de sécurité se fait selon les quatre étapes suivantes :

A

•Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;

B

•Élaborer des règles et des procédures à mettre en oeuvre dans les différents services de l'organisation pour les risques identifiés ;

C

•Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;

D

Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace

Questions?