Université
De Ouargla

Département d'Electronique et de télécommunications

Chapitre 1. Introduction à la sécurité de l'information

Réalisé par : Hassiba LOUAZENE

Bibliographié

- Cour « Introduction : Sécurité des Systèmes d'Informations », Département d'Informatique et des Technologies de l'Information, Université Kasdi Merbah Ouargla
- Cour« Introduction a la sécurité Informatique », Département de physique/Infotronique IT/S6,université Boumerdes ,université de Limoges.
- Cour « Introduction à la sécurité des systèmes d'information et de communication, Ecole Nationale des Transmissions Formation Après Intégration – ITISSAL .

Chapitre 1. Introduction à la sécurité de l'information

- Systèmes d'information
- Qu'est-ce que la sécurité ?, Menaces et Attaques
- Les objectifs de la sécurité de l'information :
- Confidentialité, Intégrité, Disponibilité
- Les mesures de sécurité

Systèmes d'information

- Un **système d'information** est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler.

- Organisation des activités consistant à **acquérir**, **stocker**, **transformer**, **diffuser**, **exploiter**, **gérer**... les informations.

Qu'est-ce que la sécurité

➢**La sécurité information** c'est l'ensemble des moyens mis en œuvre pour **réduire** la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

1.Les menaces

Le système d'information doit être sécurisé par rapport à des menaces potentielles ou avérées.
Le SI d'une entreprise ou d'une organisation est plus ou moins sensible à des menaces potentielles. C'est le degré de sensibilité aux menaces potentielles. On parle alors d'une entreprise comme étant une cible potentielle compte tenu des enjeux qu'elle représente comme une banque ou une entreprise de haute technologie par exemple. Le SI d'une entreprise est plus ou moins exposé à des menaces avérées. C'est le degré d'exposition aux menaces avérées. Exemple de menaces :

1.Les menaces

- L'intrusion
- Le vol d'informations
- La falsification d'informations
- La destruction d'informations
- La mise hors service de ressources
- etc.

1.Les attaques

Une attaque correspond à la réalisation d'une menace. Une attaque est réalisée par un ou des agresseurs.

Une attaque se définit par :

- son origine (qui ou quoi)
- son commanditaire
- sa cible (qui ou quoi)
- son objectif (pourquoi)
- ses moyens (techniques, humains, organisationnels, financiers, temporels)

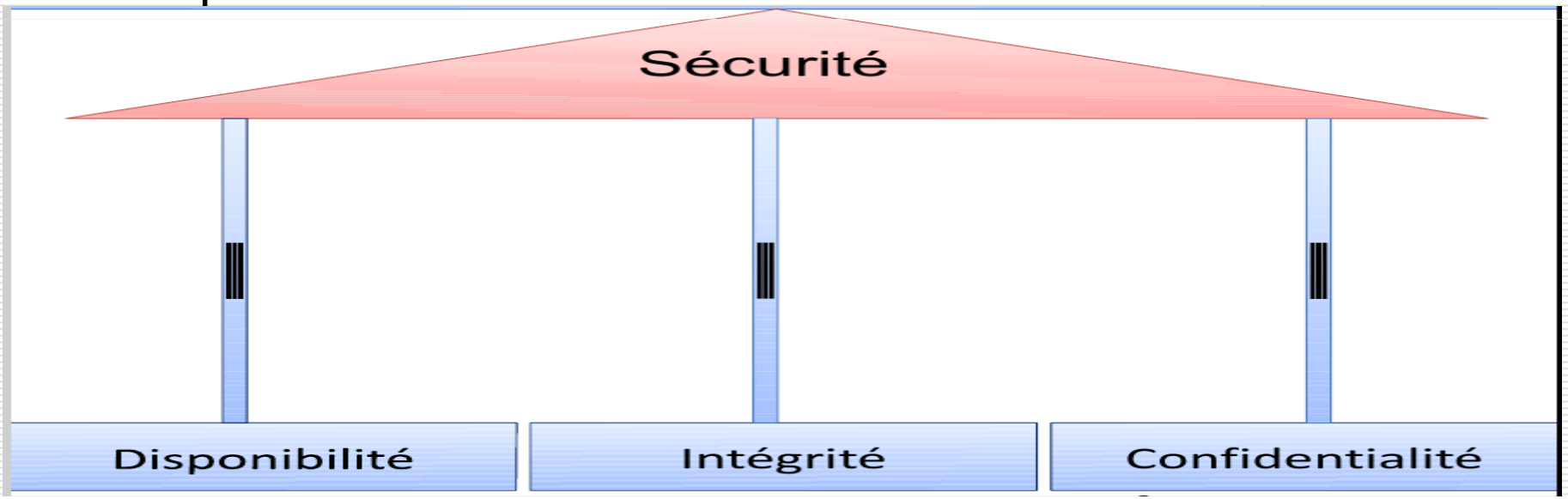
1.Les attaques

- son type (attaque par IP spoofing, par ingénierie sociale…)
- son mobile ou sa motivation (pourquoi)
- sa justification (politique, économique, philosophique, culturelle, religieuse, etc.)

Les objectifs de la sécurité de l'information

Les principaux objectifs à garantir:

– intégrité
– confidentialité
– disponibilité

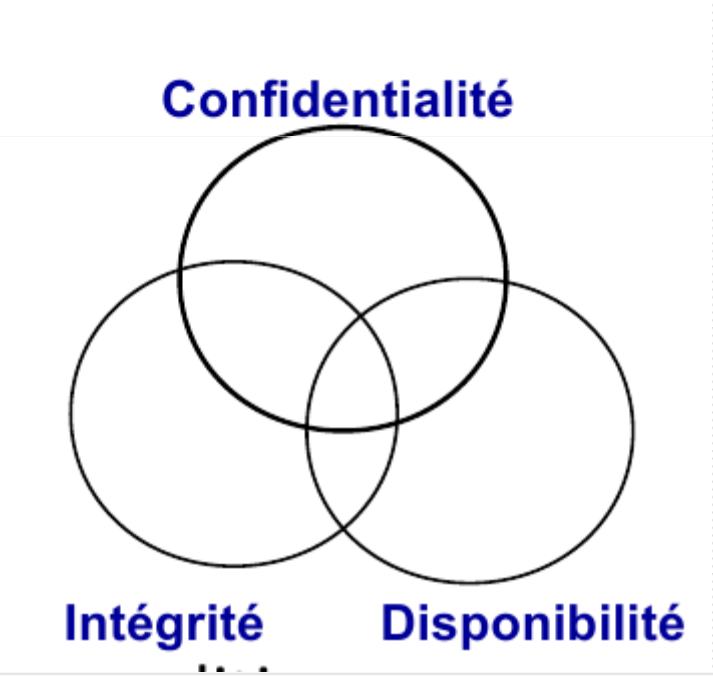


Les objectifs de la sécurité de l'information

1. Confidentialité

➢Seuls les utilisateurs habilités (autorisés) ont accès à l'information

➢ qui peut "voir" quoi?



Les objectifs de la sécurité de l'information

2. Intégrité

- Une information n'est modifiée que dans des conditions prédéfinies (selon des contraintes précises).
- Les contraintes d'intégrité : l'ensemble des règles (des assertions) qui définissent la cohérence d'un système d'information. Ex: toute règle de cohérence d'une base de données.
- L'intégrité veut dire : exactitude, précision, modifications autorisées seulement, cohérence.

Les objectifs de la sécurité de l'information

3. Disponibilité et fiabilité (pérennité)

- Terminologie du milieu de la sécurité pour caractériser le bon fonctionnement d'un système informatique.
- Un système informatique doit être disponible à ses utilisateurs autorisés selon les conditions prédéfinies.
- Présence sous forme utilisable (besoins et spécifications) satisfaisant des contraintes de temps, performance et qualité

Les objectifs de la sécurité de l'information

- La fiabilité est l'aptitude d'un système informatique à fonctionner d'une manière continue pendant une période donnée (sa durée de vie). Un système informatique ne doit pas avoir de bugs liés à des problèmes techniques de conception ou de programmation.

Étude (analyse) des risques

- Il est nécessaire de réaliser une analyse de risque en prenant soin **d'identifier les problèmes potentiels avec les solutions** avec les **coûts associés.**

- L'ensemble des solutions retenues doit être organisé sous forme d'une **politique de sécurité cohérente**, fonction du niveau de tolérance au risque.

- On obtient ainsi la liste de ce qui doit être protégé.

Evolution des risques

- Croissance de l'Internet
- Croissance des attaques
- Failles des technologies
- Failles des configurations
- Failles des politiques de sécurité
- Changement de profil des pirates

Étude (analyse) des risques

- Quelle est la valeur des équipements, des logiciels et surtout des informations ?
- Quel est le coût et le délai de remplacement ?
- Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau
- Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société ?

Étude (analyse) des risques

Il faut cependant prendre conscience que les principaux risques restent :

- « câble arraché »,
- « coupure secteur »,
- « crash disque »,
- « mauvais profil utilisateur », …

Étude (analyse) des risques
Ce qu'il faut retenir

- Inventaire des éléments du système à protéger
- Inventaire des menaces possibles sur ces éléments
- Estimation de la probabilité que ces menaces se réalisent

Le risque « **zéro** » n'existe pas, il faut définir le risque résiduel que l'on est prêt à accepter.

Établissement d'une politique de sécurité

- Il ne faut pas perdre de vue que la sécurité est comme une chaîne, guère plus solide que son maillon le plus faible

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

Établissement d'une politique de sécurité

Suite à **l'étude des risques** et avant de mettre en place des **mécanismes de protection**, il faut préparer une politique à l'égard de la sécurité.

Une politique de sécurité vise à définir les moyens de protection à mettre en œuvre

Établissement d'une politique de sécurité

- Identifier les risques et leurs conséquences.
- Elaborer des règles et des procédures à mettre en œuvre pour les risques identifiés.
- Surveillance et veille technologique sur les vulnérabilités découvertes.
- Actions à entreprendre et personnes à contacter en cas de détection d'un problème.

Établissement d'une politique de sécurité

- Quels furent les coûts des incidents informatiques passés ?
- Quel degré de confiance pouvez-vous avoir envers vous utilisateurs interne ?
- Qu'est-ce que les clients et les utilisateurs espèrent de la sécurité ?
- Quel sera l'impact sur la clientèle si la sécurité est insuffisante, ou tellement forte qu'elle devient contraignante ?

Établissement d'une politique de sécurité

- Y a-t-il des informations importantes sur des ordinateurs en réseaux ? Sont-ils accessible de l'externe ?

- Quelle est la configuration du réseau et y a-t-il des services accessibles de l'extérieur ?

- Quelles sont les règles juridiques applicables à votre entreprise concernant la sécurité et la confidentialité des informations ?

Établissement d'une politique de sécurité

Mise en œuvre

- Audit
- Tests d'intrusion
- Détection d'incidents
- Réactions
- Restauration

Merci