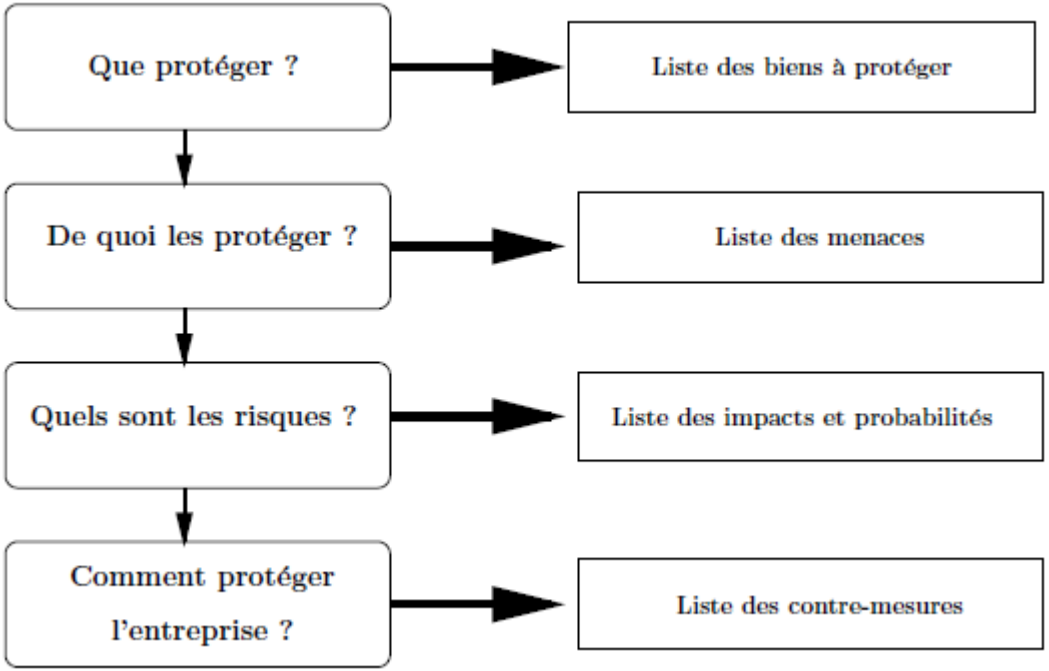
Module Sécurité Informatique (F332)

Cours 2- Enjeux de la sécurité Informatique

Introduction

DEMARCHE NORME ISO 17799



Quelques concepts(1)

Menace: est une cause potentielle d'incident, qui peut résulter en un dommage au système ou à l’entreprise

Vulnérabilité: représente les failles, les brèches dans le système, tout ce qui expose le système à la menace

Attaque: Action malveillante qui tente d’exploiter une vulnérabilité dans le système et de violer un ou plusieurs besoins de sécurité

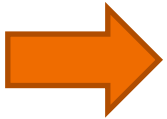
Quelques concepts(2)

Intrusion: Opération qui consiste à accéder, sans autorisation, aux données d'un système **informatique** ou d'un réseau, en contournant ou en désamorçant les dispositifs de sécurité mis en place.

Contre-mesures: sont les actions mises en œuvre pour prévenir la menace, une fois qu'elle est mesurée

Pourquoi faut-il plus de sécurité informatique ?

Développement d'internet



de plus en plus d'organismes ouvrent leur systèmes d'informations à leurs partenaires (fournisseurs , clients, …)

il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information

Objectifs de la Sécurité Informatique

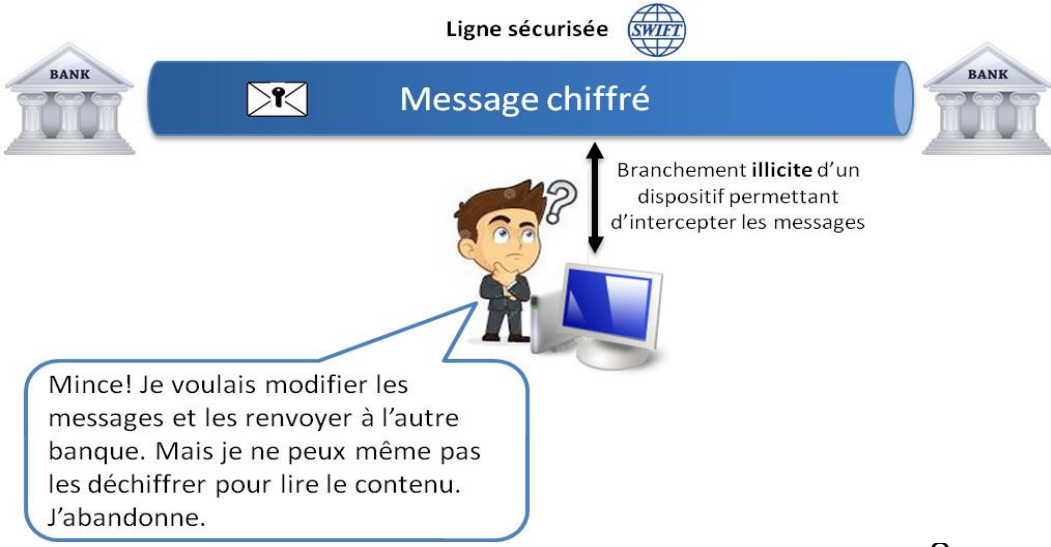
La sécurité d'un système repose sur cinq grands principes:

- ❑ Intégrité des données
- ❑ Confidentialité des données
- ❑ Disponibilité des ressources
- ❑ Authentification des utilisateurs
- ❑ Non répudiation des données

Objectifs de la Sécurité Informatique

L'intégrité des données: il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication.

La confidentialité : seules les personnes habilitées doivent avoir accès aux données.
Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées,
seuls les acteurs de la transaction possédant la clé de compréhension.



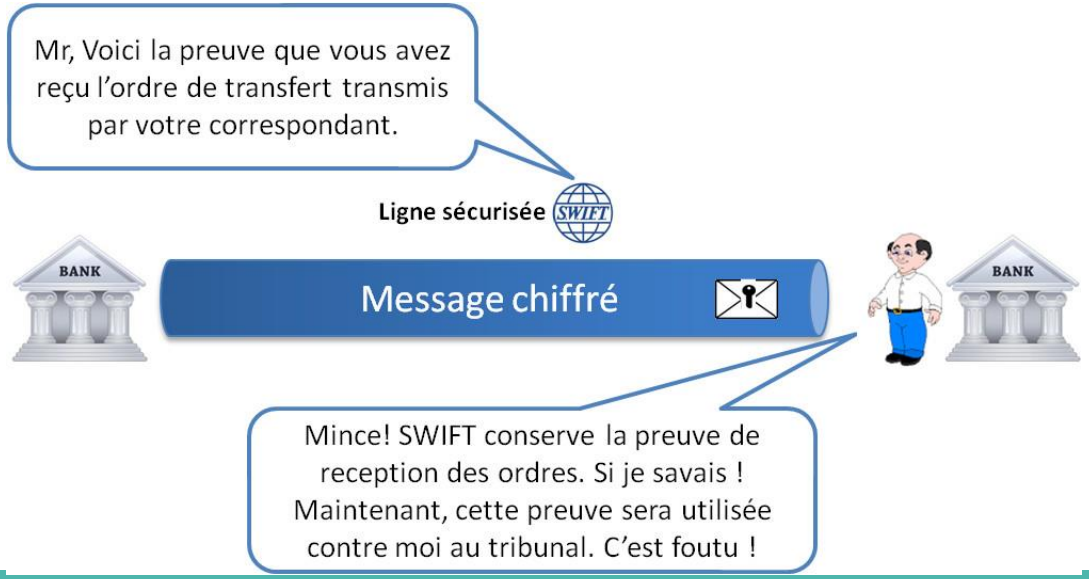
Objectifs de la Sécurité Informatique

- **La disponibilité:** il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment.

- **L'authentification :** elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

Objectifs de la Sécurité Informatique

La non-répudiation des données : une transaction ne peut être niée par aucun des correspondants. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues.



Mise en place d’une politique de sécurité

La sécurité informatique, n’est pas qu’un mot de passe !

Il est inutile de blinder la porte alors que les fenêtres sont ouvertes !

Il est nécessaire d’entreprendre la sécurité informatique dans un cadre global : il faut une politique de sécurité

Mise en place d’une politique de sécurité

Dans un contexte global, la sécurité doit être assurée:

- **au niveau utilisateur**: les acteurs doivent comprendre l'importance de leur position.
- **au niveau des technologies utilisées**: elles doivent être sûres et ne pas présenter de failles.
- **au niveau des données en elles-mêmes**: avec une bonne gestion des droits d'accès (authentification et contrôle) l'utilisateur doit posséder uniquement les droits qui lui sont nécessaires.

Mise en place d’une politique de sécurité

- **au niveau physique** (accès à l'infrastructure, au matériel): rien ne sert de sécuriser un système logiquement si matériellement l'accès à la salle des machines n'est pas sécurisé.

Mise en place d’une politique de sécurité

Démarche de mise en place d’une politique de sécurité:

1. Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences
2. Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
3. Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
4. Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

Mise en place d’une politique de sécurité

Analyse des besoins: Une telle analyse consiste tout d’abord à identifier les ressources ou les biens vitaux de l’entreprise. Ces derniers peuvent être de plusieurs ordres :

• matériel (ordinateurs, équipements réseau, etc.) ;

• données (bases de données, sauvegardes, etc.) ;

• logiciels (sources des programmes, applications spécifiques, etc.) ;

• personnes (salariés, personnel en régie, etc.).

Mise en place d’une politique de sécurité

Analyse de risque: Une fois les éléments critiques identifiés, il convient, pour chacune des ressources vitales, d’associer les trois éléments menace, vulnérabilité et conséquences, qui visent à définir l’analyse de risques proprement dite, telle que définie par l’ISO comme la combinaison de la probabilité d’un événement et de ses conséquences.

Risque=conséquence x probabilité d’occurence

Mise en place d'une politique de sécurité

Analyse de risque: consiste à répertorier les risques possibles, estimer leur probabilité et leur coût (dommages).

- Les risques ayant une occurrence faible et une conséquence faible sur l'entreprise ne sont pas pris en compte *a priori*. On peut cependant mitiger ce point par le fait que la combinaison de risques faibles peut engendrer un risque fort. Ils doivent donc être pris en compte.

Mise en place d'une politique de sécurité

- Les risques ayant une occurrence forte et une conséquence forte ne doivent pas exister par nature, car ils mettraient en cause les activités de l'entreprise. Si de tels risques existent, il est probable que les coûts nécessaires pour les réduire seront trop importants pour l'entreprise. Il est donc nécessaire de faire appel à des assurances pour les couvrir.

- Les risques ayant une occurrence forte et une conséquence faible doivent être pris en compte et faire l'objet d'une analyse coût/acceptation du risque.

Mise en place d'une politique de sécurité

- Les risques ayant une occurrence faible et une conséquence forte doivent être pris en compte et faire l'objet d'une analyse coût/acceptation du risque. Il est probable qu'il faille faire appel à des assurances pour les couvrir.

- Tous les autres cas doivent être pris en compte et faire l'objet d'une analyse coût/acceptation du risque.

Bien que la sécurité absolue n'existe pas en soi, l'entreprise détermine le niveau de risque qu'elle est prête à accepter sur ses ressources en comparaison avec le coût induit par les menaces qu'elle encourt.

Quelques Méthodes d'Analyse de Risque

1. MARION (*Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux*);

2. MEHARI (*MEthode Harmonisée d'Analyse de RIsques*) ;

https://www.clusif.asso.fr/fr/production/mehari/

3. EBIOS (*Expression des Besoins et Identification des Objectifs de Sécurité*), mise au point par la DCSSI (*Direction Centrale de la Sécurité des Systèmes d'Information*) ; http://www.ssi.gouv.fr/fr/confiance/ebios.html

4. La norme ISO 17799.