BTS SIO2 SLAM **Date:**11-09-2023

Chapitre1: cours sur la cybersécurité

1-1 Introduction

Quand on parle de la sécurité informatique ou cybersécurité, l'objectif n'est pas de sécuriser le matériel, l'ordinateur en réseau en lui-même, c'est beaucoup plus de protéger un système d'information.

Qu'est-ce qu'un système d'information(SI)?

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. C'est aussi l'organisation des activités consistant à acquérir, stocker, transformer diffuser, exploiter, gérer …. Les informations.

Aujourd'hui nous avons besoins de plus d'informations:

• Grande diversitée dans la nature des informations:
– données financières
– données techniques
– données médicales
– ...

Ces données constituent les biens des personnes et des entreprises et peuvent être très convoitées.

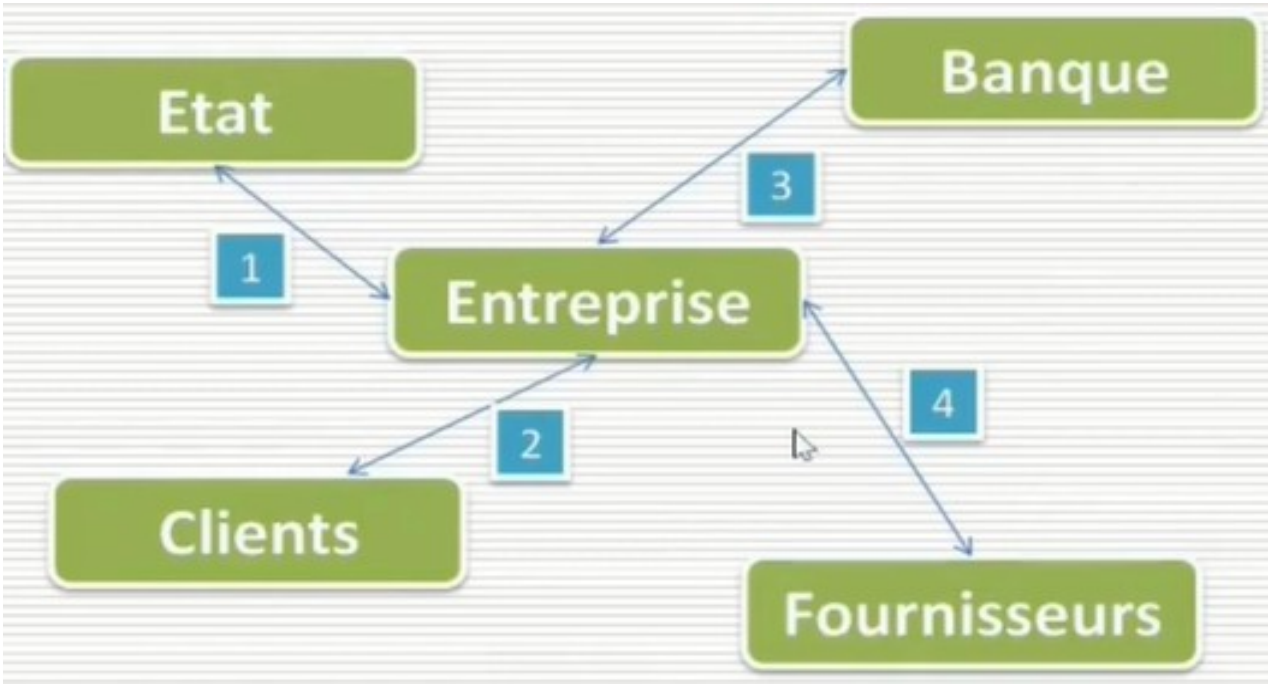
Ces données qui constituent les patrimoines des entreprises sont les cibles privilégiés des pirates informatiques.

➢Un des moyens techniques pour faire fonctionner un système d'information est d'utiliser **un système informatique (coeur)**.

➢**Les Systèmes informatiques sont devenus la cible de ceux qui convoitent l'information.**

Assurer la sécurité de l'information =→ d'assurer la sécurité des systèmes informatiques.

- **Les entreprises font face à plusieurs défis**



Les entreprises ne peuvent pas fermées complètement leur système informatique à

cause des partenaires avec qui elles doivent avoir des échanges. Ces partenaires peuvent être des banques, des clients, des fournisseurs ou l'administration. Même si l'entreprise est bien protégée de l'intérieur, elle risque toujours de récupérer des virus informatiques ou subir des actes de piratage dans les échanges de données avec les partenaires. Ces points de connexion de communication avec ces partenaires sont à surveiller. Donc l'entreprise doit veiller à la sécurisation de ces données internes et externes. Ce qui nous amène à cette définition de la sécurité informatique:

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

Nous avons **deux remarques:** la **première remarque** c'est qu'on ne vise pas à éliminer la vulnérabilité d'un système cela est quasiment impossible, mais on cherche à la réduire parce qu'il y a toujours un risque, on vise à réduire au maximum la vulnérabilité. Dans la **deuxième remarque**, on est face à deux types de

menace, des menaces intentionnelles c’est-à-dire, l’acte est prémédité, ça peut être un pirate ou un individu mal intentionné, un concurrent par exemple ou une menace accidentelle, un utilisateur mal formé et mal informé qui peut sur la clé USB ou autre support télécharger des données infectées et l’introduire dans le système informatique de l’entreprise sans s’en rendre compte. Il ne sait pas par exemple installer des logicielles donc il télécharge des jeux sur internet. On a deux types de menaces: des menaces accidentelles ou intentionnelles.

Chapitre2: Terminologie

Des mots souvent utilisés en cybersécurité:

- Actif
- Vulnérabilité
-Incident
- Menace
- Risque
- Attaque
- contre-mesures

Définitions:

1- Actifs ou assets

N'importe quoi qui a de la valeur pour l'entreprise. Ça peut être :
- des matériels
- des logiciels
- des personnes

Les actifs peuvent être des services et des protocoles réseaux, des informations stockées ou partagées, ou des informations qui circulent sur un support de transmission, ou des infrastructures d'un système d'information, tout ce qui a une valeur pour les entreprises. L'objectif pour les entreprises, c'est de protéger ces différents actifs.

2- La Vulnérabilité ou faille

C'est une faiblesse au niveau d'un actif. Par exemple une maison qui a des fissures, des portes mal sécurisées, ça représente des failles, un joueur de football ou un sportif de

haut niveau est un actif pour les clubs. s'il ne mange pas bio, ne dort pas bien, ne prend pas en compte des mesures de sécurité pour protéger sa santé et son corps, on dira qu'il est vulnérable, il a des failles, des faiblesses. De la même façon, un ordinateur est un actif, s'il ne contient pas d'antivirus ou si l'antivirus n'est pas mis à jour , si nous n'avons pas de mot de passe ou si nous utilisons des mot de passe faible. On dira que nous sommes vulnérables. On parle de **pentest**: un domaine pour étudier les failles. Par exemple on fait des tests: injection SQL, XSS (Cross-site scripting)...Etc. C'est un sous-domaine de la sécurité informatique.

3- Un incident de sécurité

C'est un dysfonctionnement signalé par un utilisateur sur un actif. Dans le cas d'un sportif, ça peut être une blessure ou une maladie. Dans le cas d'un ordinateur, soit il est piraté ou victime d'un virus informatique.

4- Menace de sécurité

C'est une cause potentielle d'incident: tout ce qui peut exploiter une vulnérabilité sur actif pour enfreindre la sécurité. Il peut entraîner des dommages très sérieux sur actifs si cette menace se concrétisait. Cette menace n'est pas encore réalisée. C'est une possibilité, une probabilité. Dans le cas de l'informatique, on dit que notre actif court une menace parce qu'il n'a pas d'antivirus ou l'antivirus n'est pas mis à jour. Une menace est la cause d'un incident. C'est l'exploitation d'une faille de sécurité.

5- Risque

C'est la probabilité de voir une menace informatique se transformer en événement réel entraînant une perte.
Risque = Menace x Vulnérabilité x Actif . Le risque c'est la

probabilité. La probabilité que la menace se concrétise réellement.

6- Attaque informatique

C’est une action volontaire et malveillante visant à causer un dommage aux actifs. C’est la concrétisation d’une menace, et nécessite l’exploitation d’une vulnérabilité. Par exemple notre ordinateur est piraté (hacked). La menace s’est transformée en événement réel.

7- Contre-mesure

C’est une mesure de sécurité informatique défensive, prenant la forme d’une technique, d’un dispositif, d’une procédure, et dont le but est de s’opposer à un incident, de contrer une attaque susceptible de porter atteinte aux actifs. De manière générale, on parle des contre-mesures préventives et des contre-mesures correctives. Les contre-mesures préventives, on va simuler les actions avant qu’elles n’arrivent, et correctives, c’est comment on agit après que la menace s’est concrétisée.

Le pentest, ou **test d'intrusion**, est une **méthode visant à évaluer la sécurité d'un système informatique en simulant une attaque**. L'objectif est d'identifier les vulnérabilités et les failles de sécurité qui pourraient être exploitées par un attaquant malveillant.