# Première année

# Cours 2: Les risques et menaces

---

Système d'Information (S.I) – > **Ensemble des ressources destinées à collecter, classifier, stocker, gérer, diffuser les informations au sein d'une organisation**. *Le S.I doit permettre et faciliter la mission de l'organisation.*

La sécurité réduit les risques et limite leurs impacts, elle consiste à assurer la sécurité de l'ensemble des biens.

## Les risques:

- **accidents naturels:** incendie, dégâts des eaux, etc...
- **perte des services essentiels:** coupure courant, réseau, rupture de stocks
- **erreurs:** tous les secteurs d'activité (analyse, conception, utilisation, ...)
- **malveillance:** vol, vandalisme, fuite d'informations

## Classification du risque:

1. **Nul: risque jugé non significatif**
2. **Faible: événement générant une nuisance organisationnelle, des pertes financières faibles, peu gênant pour l'utilisateur**
3. **Sensible: événement occasionnant des pertes financières significatives, nuisible à l'image, gênante pour l'utilisateur**
4. **Critique: événement occasionnant des pertes financières inacceptables, une perte de clientèle**
5. **Stratégique: événement susceptible d'entraîner un arrêt immédiat d'une activité de l'entreprise**

## Les différents types de menaces:

- **La cybercriminalité** – > comprend des acteurs isolés ou des groupes qui ciblent des systèmes pour des gains financiers ou pour causer des perturbations.
- **Les cyberattaques** – > impliquent souvent la collecte d'informations pour des raisons politiques.
- **Le cyberterrorisme** – > vise à affaiblir les systèmes électroniques pour entraîner la panique ou la peur.

## Exemples des différents types d'attaques:

- Programme malveillants
- Injection SQL
- Attaque par phishing

- Attaque de l'homme du milieu
- Attaque par déni de service
- Attaque par mot de passe

## Il existe de nombreux types de programmes malveillants:

- **Virus** – > **programme** qui se duplique en s'attachant à un fichier afin de **se propager dans tout le système**
- **Cheval de Troie** – > **programme** qui **se fait passer pour un logiciel authentique**, son but: endommager ou collecter des données
- **Spyware** – > **programme** espion qui **enregistre les actions d'un utilisateur**
- **Ransomware** – > **malware** qui **verrouille les fichiers et les données de l'utilisateur sous menace et demande de rançon**
- **Adware** – > **logiciel publicitaire** qui peut être utilisé pour propager un malware
- **Botnets** – > **réseaux d'ordinateurs infectés par des malwares**, ils effectuent des tâches en ligne sans l'autorisation de l'utilisateur

Injection SQL (Structured Query Language): type de cyberattaque utilisé pour **contrôler et voler les données d'une base de données**. Les cybercriminels exploitent les vulnérabilités dans les applications orientées données pour insérer du code malveillant dans une base de données.

Attaque par phishing: les cybercriminels envoient des **e-mails qui semblent provenir d'une entreprise légitime pour demander des informations sensibles aux victimes**.

Attaque de l'homme du milieu: cyberattaque qui consiste à **intercepter la communication entre deux individus** pour leur voler des données.

Attaque par déni de service: les cybercriminels **empêchent un système informatique de répondre à des requêtes légitimes en surchargeant les réseaux et les serveurs avec du trafic.**

Attaque par mot de passe: les cybercriminels essaye de s**e connecter à un compte en entrant un mot de passe construit.**

Attaque par force brute: le **mot de passe est cassé en testant tous les mots de passe possibles.**

Attaque par dictionnaire: le **mot de passe est craqué en testant des mots se trouvant dans les dictionnaires.**

Attaque hybride: **force brute + dictionnaire**