

◆ **Rapport de cours**  
**Jour 1**

Victoria SAUTEREAU

**E  
S  
T  
I  
A  
M**

**Cybersécurité**



École d'informatique  
et du numérique

2ème année  
2022/2023




# Sommaire

## **Partie 1 : Le cube magique de la cybersécurité**

- Les principes de la sécurité
- Les états des données
- La politique de sécurité
- Les contre-mesures de cybersécurité

## **Partie 2 : Les menaces pour la cybersécurité**

- Les types de malwares
  - Les principes de l'ingenierie sociale
  - Les menaces d'ingenierie sociale
  - Les Types de cyber-attack
- 

# Partie 1 : Le cube magique de la cybersécurité

## • Les principes de la sécurité

- La confidentialité : Les systèmes et les données ne sont accessibles qu'aux utilisateurs autorisés.
- Intégrité : Les systèmes et les données sont fiables et complets.
- Disponibilité : Les systèmes et les données sont accessibles quand on en a besoin.

## • Les états donnés

- Données au repos ou stockées: désigne les données qui ne sont pas accessibles et qui sont stockées sur un support physique ou logique (d'enregistrements dans des bases de données, de documents...)
- Données en transit : Les données qui transitent par un courrier électronique, un site web, des applications de travail collaboratif telles que Slack ou Microsoft Teams, une messagerie instantanée ou tout type de canal de communication privé ou public.
- Données en cours de traitement: Lorsqu'elles sont ouvertes par une application et consommées ou consultées par les utilisateurs.

## • La politique de sécurité

- Politiques d'identification et d'authentification
  - Stratégies de mot de passe
  - Règles de bon usage
  - Politiques d'accès à distance
  - Politiques de maintenance du réseau
  - Politiques de gestion des incidents
-

# Partie 2 : Les menaces pour la cybersécurité

## • Types de malwares

- Le « malware » (ou programme malveillant) désigne un logiciel conçu pour perturber le bon fonctionnement d'un ordinateur ou obtenir l'accès à des systèmes informatiques à l'insu ou sans l'autorisation de l'utilisateur.
  - Cheval de Troie: Malware qui effectue des opérations nuisibles sous couvert d'une opération souhaitée.
  - Bombe logique: Programme malveillant qui utilise un déclencheur pour réactiver le code malveillant.
  - Virus: Code malveillant exécutable joint à un autre fichier exécutable, comme un programme légitime.
  - Rootkit: Code malveillant utilisé pour compromettre un système à l'aide de portes dérobées.
  - Ransomware: Code malveillant retenant un système informatique (ou les données qu'il contient) captif jusqu'à ce que la cible paye une rançon.
  - Ver: Code malveillant qui se reproduit en exploitant indépendamment des vulnérabilités dans les réseaux.
  - Whaling: Utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter les données privées des dirigeants d'une entreprise, comme des informations d'identification.
  - Piratage de navigateur : Code malveillant qui modifie les configurations du navigateur.
  - Phishing: Utilisation des e-mails, de la messagerie instantanée ou d'autres médias sociaux pour tenter de collecter des données privées, comme des informations d'identification, en se faisant passer pour une personne fiable.
  - Pharming: Utilisation d'un site web pour tenter de collecter des données privées, comme des informations d'identification, en se faisant passer pour un site web fiable.
  - Logiciel espion/logiciel publicitaire : Code malveillant transmis par e-mail ou téléchargé à partir du web, capable de collecter des informations utilisateur ou d'installer des bannières publicitaires dans des programmes, des navigateurs web ou des pages web.
  - Courrier indésirable : Spam ou courrier indésirable, utilisé pour envoyer des publicités, des liens malveillants, un malware ou des contenus trompeurs..
-

- **Les principes de l'ingénierie sociale**

- L'urgence:Escroquerie encouragée par la croyance qu'il reste de temps pour agir
- L'intimidation :Utilisation d'intimidations ou de menaces pour convaincre.
- L'autorité:Utilisation d'un pouvoir ou d'une capacité de persuasion.
- La familiarité/le lien:Utilisation des liens avec la victime pour établir une relation de confiance.
- La rareté:Escroquerie encouragée par la croyance qu'il reste seulement une quantité limitée.
- Le consensus ou la preuve sociale:Escroquerie encouragée par les croyances et les actions des autres

- **Les menaces de l'ingénierie sociale**

- Usurpation d'identité:Prétendre être quelqu'un d'autre pour gagner la confiance d'une personne ou accéder aux zones ou données non autorisées
  - Espionnage par-dessus l'épaule (Shoulder Surfing):Observer une victime pendant qu'elle saisit son code au distributeur automatique.
    - Canulars:Utiliser la tromperie pour provoquer la réaction irrationnelle d'un utilisateur
    - Accès non autorisés :Suivre une personne autorisée pour accéder à un emplacement sécurisé ou à une zone restreinte
    - Dumpster Diving :Récupérer des documents dans une poubelle ou un conteneur de recyclage
-

## • Les types de cyber-attack

La Menace de type « zero-day »: Attaque tentant d'exploiter des failles logicielles qui sont inconnues ou non divulguées par l'éditeur du logiciel.

Repérage: Type d'attaque qui examine tout le trafic réseau qui transite par la carte réseau, même s'il n'est pas adressé au système.

- Man-in-the-Middle: Type d'attaque qui intercepte les communications entre les ordinateurs pour voler des informations pendant qu'elles transitent sur le réseau.
- Enregistreur de frappe: Programme utilisé pour conserver ou enregistrer les frappes de touche de l'utilisateur sur un système.
- Dos et DDoS: Type d'attaque qui refuse l'accès aux utilisateurs autorisés, rendant inaccessibles le réseau, les services réseau ou les données sur le réseau.
- Mystification: Type d'attaque qui utilise l'emprunt d'identité pour tirer parti d'une relation de confiance entre deux systèmes.
- Phishing vocal :Utilisation de communications vocales pour tenter de collecter des données privées,comme des informations d'identification, en se faisant passer pour une personne fiable.

## • Les types de cyber-attack : application et web

- Dépassements de mémoire tampon: Attaque d'application ou web qui transmet intentionnellement une quantité excessive de données surchargeant la mémoire conçue pour recevoir les entrées.
  - Exécutions de code à distance: Attaque d'application ou web qui établit un accès distant à un programme, un service ou un appareil.
  - Injections XML/SQL: Attaque d'application ou web qui exploite les défaillances pour valider les requêtes de bases de données.
  - Contrôles ActiveX et Java: Attaque d'application ou web qui exploite l'hôte distant en installant des plug-ins de programmes malveillants.
-