5.01 - Introduction à la cybersécurité

Durée approximative : ***2h***

Eléments du référentiel adressé :

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R1 : Accompagnement du client***
    - ***C04 - Analyser un système informatique***
      - ***Acteurs de l'écosystème réglementaire, normatif et de référence des bonnes pratiques***
      - ***Méthodologie de recherche et d'analyse de documentation y compris en anglais***

- ***U6 - Valorisation de la donnée et cybersécurité***
  - ***D1 : Elaboration et appropriation d'un cahier des charges***
    - ***C05 -Concevoir un système informatique***
      - ***Usages et documents réglementaires, normatifs adoptés au sein de l'entreprise et du secteur de la sécurité des systèmes d'information***

I. Le paysage de la cybersécurité

Définir les types de hacker.

- White hat
- Grey hat
- Black hat

Faire un tour d'horizon des sources de menaces :

- cybercriminalité (extorsion de fond, destruction brute, activités de réseau)

- terrorisme (risques terrorise et écoterroriste, militants écologiques ou politiques, attaque sur des infrastructures vitales)
- Espionnage industriel ou étatique (concurrent malveillant ou puissance étrangère)
- Cyberguerre (acte de guerre de la par d'une puissance étrangère)

Evoquer l'industrialisation de la menace. Le fait que les actions sont de moins en moins commises par des pirates isolées, mais de plus en plus par des réseaux structurés, utilisant principalement des robots et des méthodes d'industrialisation des attaques.

> **Conseil** : illustrer le propos avec des captures de trames ou des logs de pare feu sur une interface publique.

> A titre individuel, lorsque je faisais de l'hébergement chez moi (2023 à 2025), c'était en moyenne 400 à 600 tentatives par jours. Essentiellement des actions automatisées à large échelles, effectuées par des robots qui scannaient à longueur de temps la moindre faille. Ce n'est qu'en cas de succès de ces opérations qu'un humain prends la relève.
>
> *- Chabran Olivier*

Terminer sur les objectifs des pirates, les deux principaux sont :

- Voler ou extorquer de l'argent
- Rendre des services inaccessibles ou inopérants
- Voler des données confidentielles, qui aujourd'hui, valent bien plus que l'argent en lui même.

II. Les principales attaques

> **Une chaîne n'a que la force de son maillon le plus faible.**

> *- Olivier Lajous, "L'art de diriger ?"*

De nombreuses attaques ciblent les systèmes. Les principales qui ciblent les systèmes sont :

- Attaque par DDoS
- tentatives d'intrusion
- ransomwares

Mais vu que les systèmes sont de plus en plus protégés, la cible privilégiée est l'élément humain : l'utilisateur

- Phishing
- Malwares
- ransomware
- Social engineering

Concernant les vecteurs d'attaques (messagerie, wifi public, clé USB), présenter les vecteurs et leur méthodologie d'exploitation.

> **Conseil** : Utiliser des échantillons de mails, un résultat de scan wifi wireshark et des clé USB pour illustrer le propos.

Expliquer les méthodes de préventions utilisées pour la correction de ses points.

- Campagnes de phishing
- Politique de traitement des clé USB trouvées
- utilisation d'un VPN, préférer les partages de connexion 4G au wifi public si possible.

III. Le rôle grandissant de l'IA dans la cybersécurité

Evoquer l'utilisation de l'IA dans la recherche et la protection des menace.

Evoquer également son pendant en terme de développement et d'automatisation des attaques utilisé par les pirates.

IV. Les acteurs règlementaires et normatifs

En réponse aux menaces et aux dérives quand au traitement de la donnée par les GAFAM et autres, une série d'organisme a vu le jour.

Ceux-ci sont en charge de gérer les aspects règlementaires, législatifs et normatif quand à la sécurité informatique et le traitement des données.

- CNIL
- ANSSI
- Cybermalveillance
- CVE Foundation
- CERT-FR

> **TP** : Sur le site de l'anssi, chercher et télécharger les guides de bonnes pratiques. Analyse et débat en classe.

Conclure sur le rôle de "white hat" de l'étudiant.

> **Evaluation** : faire signer le contrat de prestation cyber aux étudiants.

Ressources associées :

Les types de hackers et principes d'attaques

Etat des cybermenaces (2025)

Revision #1
Created 2026-07-17 13:12:02 UTC by Olivier
Updated 2026-07-17 13:12:02 UTC by Olivier