Atelier FFCYB - 02/10/2023

La cyber demain, notre vision :

Comment s'imaginer dans la cyber & pdv ?

Constat:

Indispensable pour le présent et le futur contre des attaques

Invisible pour une grande partie du public

Inconscient sur l’importance de leurs données personnelles,

Stéréotype sur les personnes travaillant dans la cyber

Phishing touchent plus les personnes de moins de 30 ans car elles vont plus vite, ne prennent pas le temps de réfléchir. -> Vérifier le mail avant de cliquer.

81% des attaques sur les entreprises commencent par un mail de phishing

50% des tpe/PME déposent le bilan suite à une cyberattaque

Coût de la cybercriminalité:

6,2 trillions en 2021

25 trillions en 2025

Un enjeux:

Cyberspace, protection des données, entreprises contre les cyber attaques

Créer des outils sans faire payer le prix coûtant

Partage des données sur internet de façon sécurisée

Gouvernance, et l’éthique très importante

Définition:

Cyber vient du mot gouverner -> S’applique dans différents environnements

Pas juste un axe de compétence

Connection internet c’est la connection à l'univers du monde

Dissocier les métiers cyber/autres, c’est au spécialiste du cyber de sensibiliser les autres métiers face au risque cyber. Bien souvent les spécialistes refusent de le faire car c’est un travail fastidieux.

Compréhension de:

Tentative d’intrusion -> cyber attaque -> Pour ça que la cybersécurité existe

Psychologie de l’attaquant, Comment empêcher un cyber attaquant de jouer de la naïveté d’une personne

Beaucoup de cyber attaque dans l’interne d’une entreprise

Groupe de hacker sur darkweb qui collaborent ensemble et sont reliée à une cause, base de social engineering

Beaucoup de recherche et compréhension de comment les choses fonctionnent pour attaquer/défendre. Ex social hardware. Comment le détourner

Un moyen :

Choisir sa branche:

Liée à sa manière de travailler

Au appétence

L’évolution professionnelle

Travail d’équipe:

Sensibilisation

Plusieurs opinions différents

Echanges

Répartir les tâches

Pôles différents

Plusieurs sujets différents

Transverse

Travail d’interaction

Travail seul = Impossible

Les divers métiers:

Dev

Pentests

Architecture réseau

Cryptographe

Data scientist

R&D:

Vérifier que le code est sécurisé

Bibliothèque piégée ?

Methodo security by design

Cryptographie:

Polytechnique -> Confiée au département spécialisée de polytechnique

Architecture réseau:

Inventaire

Version

Architecture

Applicatif

Réseau

Vieux système mis en place mais nécessaire au bon fonctionnement d’une entreprise, il faut donc faire avec ( Entreprise qui utilisent windows NT )

Blockchain:

Smart contract: Contrat signé par des NFT dans le WEB.3, permet de savoir grâce au wallet qui a utilisé le NFT qui a signé, et l'horodatage (date, heure) de quand nous avons utilisé ce NFT. Autrement dit Signature électronique avancé

Approche cybersécurité:

Problème WEB.3: Nom de domaine ont déjà été piraté, donc il existe du détournement de nom de domaine. (Site malveillant)

Data scientist:

Permet de faire de l’ia en cyber.

Deep learning:

Plusieurs neurones ( grappes de neurones )

Une neurones qui dispatch a d’autres neurones