**Cyber security**

Def : la protection d’un systeme en réseau et de données contre une utilisation non autorisé ou un méfait .

Les données personnelles : est toute info se rapportant á une personne physique identifiée ou identifiable

* *Identité offline* : avec laquelle on intéragit á la maison , á l’ecole ou au travail
* *Identité online* : quand on est dans des cyberspaces par exemple : nom user ou alias , doit etre adapté et respectueux

Quelles sont nos données : dossiers médicaux , scolaires, financiers **=> Se trouve dans <=** dossiers médicaux , cartes de fidélité de magasins , photos en ligne , appareils info.

Les données entreprises :

Les types de données d’entreprises :

* Données traditionnelles : personnelles , intellectuelles , financiers
* Internet des objets et Big Data : IOT , big data

Objectifs des données de l’entreprise ( de la cyber securité) :

* Confidentialité : le message envoyé doit etre chiffré
* Integrité : le message envoyé ne doit pas etre modifié que si avec les personnes autorisés ( pour assurer l’ integrité c ‘est avec la technologie la signature , l’emmetteur doit faire un hash au message envoyé et le recepteur vérifie l’intensit’e du msg ).
* La disponnibilité : accessibilité des infos .

Impact d’une faille :

*Les conséquences d’une brèche dans la sécurité:* reputation ruinée , vol de données , perte de chiffre d’affaire.

*Example :*

* Last Pass : Gestionnaire des mdp
* Vtech : fabriquant de jouets technologiques pour enfants
* Equifax : une agence d’évaluation des crédits á la consommation

La guerre cybernétique : conflit lié á l’utilisation de l’espace cybernétique .

*Expl :* stuxnet c’est pour endommager l’usine d’enrichessement nucléaire de l’iran , cree par la nsa

Objectif et avantage de cette guerre :

Gagner un avantage sur les adversaires , saboter les infrastructures

Les cyberspaces :

Sites web et puissance des données , entreprises puissantes : google ,apple , amazon, facebook

Spécialistes de la cybersécurité ( les outils pour contrer la cybercriminalité) : normes ISM , nouvelles lois ,BD de vulnérabilités , systèmes d’alerte , partage d’info sur la sécurité informatique

Menaces : c’est la possibilité d’exploiter une vulnérabilité par un attaquant , peuvent toucher les données traditionnelles

Une vulnérabilité informatique faiblesse qui peut etre exploité par les autres

L’espace de l’entreprise est divisé en plains secteurs : productioon , distribution d’energie , communication , sys de transport .

Les forces obscures :

* Menaces -> Interne (liés aux collaborateurs) , externes ( liés au cybercriminels)
* La vulnérabilitédes terminaux mobiles : BYOD ( bring your own device)
* L’emergence de l’internet des objets IOT : un ensemble de techno permettant de connecter différents appareils
* Impact du big data

Les états des données :

* Données enregistrées :sont les données au repos
* Données de transit : envoie des infos d’un appareil á un autre ( sneaker net : un support amovible , reseau filaire et sans fil)
* Données enregistrées : RAID qui a une performance aux pannes améliorées
* Données en cours de traitement : les données lors de la saisie initiale , de la modification , du calcul ou de la sortie

Les mesures de la cybersecurity :

* Des protections techno basées sur le réseau : VPN reseau virtuel qui utilise internet ,NAC , la sécurité du point d’accès sans fil
* Des protections techno logicielles
* Des protections techno matérielles
* Des protections techno dans le cloud