Chapitre01 : Concepts de base

1) Pourquoi sécuriser ?

- L'informatique est devenue un outil incontournable dans l'entreprise
- Le réseau de l'entreprise qui met en œuvre des données sensibles.
- Impossible de renoncer aux bénéfices de l'informatisation (Isoler le réseau, retirer les données confidentielles).
- Les données sensibles du SI de l'entreprise sont donc exposées aux actes de malveillance .
- **Une protection juridique faible (Les malfaiteurs sont difficilement identifiables,Les attaques sont souvent transfrontalières).**
- Les attaques sont souvent transfrontalières.
- **Des obligations légales à respecter** (Obligation de protéger les données nominatives (clients, patients, salariés, etc.), Obligation dans le cadre d'accords de partenariat (**B**usiness to **B**, secret Défense, etc.)).
- **La gravité des impacts (La survie de l'entreprise, Paralyse, Vole).**

2) Premières notions de sécurité :

a. Définition :
La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

b. Sécurité = " Safety" :
Protection des systèmes informatiques contre les accidents dus à l'environnement, les défauts du système.

c. Sécurité = "Security"*: الأمن
Protection des systèmes informatiques contre des actions malveillantes intentionnelles.

d. **La sécurité des systèmes d'information (SSI)** est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du systèmes d'information.

3) Les menaces contre les SI :

Atteinte à la disponibilité des systèmes et des données
Destruction de données
Corruption ou falsification de données
Vol ou espionnage de données
Usage illicite d'un système ou d'un réseau
Usage d'un système compromis pour attaquer d'autres cibles.

4) Le risque :

Risque = probabilité d'occurrence ×préjudice
Risque = Vulnérabilité*Menace*préjudice

Exemple :
Vulnérabilité : Clés sous le tapis
Menace :
Cambrioleur essaie d'entrer
Impact :
Cambriolage, vole de l'argent…..
Réduction de risque :
Prendre les clés avec soi

Risque résiduel :

Un pickpocket vole les clés.

5) Les menaces :

a. Menaces relevant de la sécurité de l'ordinateur et de son système d'exploitation :

- Menaces relevant de problèmes non spécifiques à l'informatique :
  - Incendie, inondation ….
  - Vol et sabotage de matériels.
  - Départ de personnes stratégiques, grève …
- Les erreurs non intentionnées :
  - Pannes, erreur d'exploitation (oublie de sauvegarde écrasement de fichiers)
  - Erreur de manipulation d'informations.

b. Menaces relevant de l'utilisation des réseaux et d'internet :

- Menaces intentionnelles :
  - Menaces passives : (Détournement des données) (Espionnage industriel et commercial, Violation déontologique, Copie de logiciel…)
  - Menaces actives : Modification de l'information (Fraude financière informatique, sabotage … Modification des logiciels Malware : bombe logique, virus, cheval de Troie, ver…

6) Types de logiciels malveillants :

a. Les virus :

Un virus est un logiciel qui s'attache à tout type de document électronique « hôtes », et dont le but est d'infecter ceux-ci et de se propager sur d'autres documents et d'autres ordinateurs.

Un virus a besoin d'une intervention humaine pour se propager.

Sur le net : (appliquettes Java ou procédures JavaScript) des programmes qui s'exécuter sur votre PC en se chargeant à distance depuis le serveur Web visité.

Exemple : Boot Sector.

b. Vers (Worm) :

Un **ver informatique** se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet en s'envoyant à travers le réseau (e-mail, Bluetooth, chat..) (Apparue en 2003)

Le ver n'a pas besoin de l'interaction humaine pour pouvoir se proliférer. Exemple : Email (Sobig.F), Réseau RPC (MSBlaster).

Objectif d'un ver :

- Espionner l'ordinateur où il se trouve ;
- Offrir une porte dérobée à des pirates informatiques ;
- Détruire des données sur l'ordinateur où il se trouve ou y faire d'autres dégâts ;
- Envoyer de multiples requêtes vers un serveur Internet dans le but de le saturer (déni de service).

Effets secondaires d'un vers :

- Le ralentissement de la machine infectée.
- Le ralentissement du réseau de la machine infectée.
- Le plantage de services ou du système d'exploitation de la machine infectée.

Exemple de ver :

Un **ver** GSM se reproduit en s'envoyant à un autre téléphone mobile par moyen Bluetooth ou MMS.

c. SPAM :

Le spam est du courrier électronique non sollicité envoyé a un très grand nombre de personnes sans leur accord préalable. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

Objectif : La publicité, Escroquerie.

d. Cheval de Troie :

Programme bénin (jeux, documents…) cachant un autre programme.
Lorsque le programme est exécuté, le programme caché s'exécute aussi et pourrait ouvrir une « porte cachée ».
Conséquences de cette attaque :

- contrôle du PC de l'extérieur
- perte de données
- divulgation de données privées (chat, e-mails …)
- espionnage: microphone, webcam
- attaques à partir du PC « infecté » (Zombi)

e. **Ransomware** ou **Rançongiciel** :

Logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. ….

7) Lutte contre les malveillances informatiques :

a. Limitez vos droits !

- GSM: Ne laissez pas Bluetooth allumé en permanence
- PC: Coupez Internet si vous ne surfez pas.
- PC: Créez un utilisateur SURF avec des droits limités.

b. Activez la fonction « Automatic Updates »

c. Anti-virus

d. *Personal firewall* Un pare feu (mur de feu) :

Est un logiciel qui forme une barrière impénétrable autours de l'ordinateur, il permet :

- D'autoriser la connexion (*allow*)
- De bloquer la connexion (*deny*) ,
- De rejeter la demande de connexion sans avertir l'émetteur (*drop*).

Quelques fonctions d'un firewall :

- Système proactif/réactif avec fonctions additionnelles
- Permets de contrôler les accès Internet de programmes spécifiques.
- Fonctions additionnelles : Filtre de processus, Anti Spam etc.

8) Les différents niveaux de sécurité :

- Sécurité physique : Relative à la protection des locaux et des machines

- Sécurité du personnel : Relative à la protection physique des employés et à la protection du S.I. de l'entreprise contre ses employés
- Sécurité des communications : Relative à la protection du système de communication(réseau)
- Sécurité des opérations : Relative à la protection des échanges de données et des systèmes informatiques.

9) La politique de sécurité :

Avant toute mise en place de procédures visant à améliorer la sécurité d'un organisme, il faut procéder à une analyse des risques et de rédiger une politique de sécurité .

- **Définition :** Un ensemble de règles formalisées auxquelles les personnes ayant accès aux ressources technologiques et aux S.I. d'une organisation doivent se soumettre.
- Deux philosophies pour la mise en place d'une politique :
  - **Prohibitive :** tout ce qui n'est pas explicitement autorisé est interdit.(institutions financières ou militaires)
  - **Permissive :** tout ce qui n'est pas explicitement interdit est autorisé. Ex. éducation familiale

10) Étapes types dans l'établissement d 'une politique de sécurité :

- **Identification des vulnérabilités**
  - En mode fonctionnement normal : définir tous les points faibles
  - En cas d'apparition de défaillances (*le système est fragilisé donc vulnérable*) : c'est dans ces moments qu'une intrusion peut le plus facilement réussir
- ***Évaluation des probabilités associées à chacune des menaces***
- ***Évaluation du coût d'une intrusion réussie***
- ***Choix des contre mesures***
- ***Évaluation des coûts des contre mesures***
- ***Décision***

11) Composantes d'une politique de sécurité

- Politique d'achat
- Politique de confidentialité
- Politique d'accès
- Politique de responsabilité
- Politique d'authentification
- Politique d'audit et de reporting

12) Les services de la sécurité :

- ❑ Authentification
- ❑ Identification
- ❑ Intégrité
- ❑ Non-répudiation
- ❑ Confidentialité

L'authentification : est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité afin d'autoriser l'accès de cette entité à des ressources(systèmes, réseaux, applications...).

- ❖ L'authentification permet donc de valider l'authenticité de l'entité en question.
- ❖ Elle protège de l'usurpation d'identité

Les entités à authentifier peuvent être :

- ❖ une personne
- ❖ un programme qui s'exécute (processus)
- ❖ une machine dans un réseau (serveur ou routeur)

Dans le cas d'un utilisateur, l'authentification consiste, en général, à vérifier que celui-ci possède une preuve de son identité ou de son statut, sous l'une des formes (éventuellement combinées) suivantes :

- ❖ Ce qu'il sait (mot de passe, code PIN).
- ❖ Ce qu'il possède (carte à puce, certificat électronique).
- ❖ Ce qu'il est (caractéristique physique, voir biométrie).
- ❖ Ce qu'il sait faire (geste, signature).

La phase de vérification fait intervenir un protocole d'authentification :

- ❖ (TLS)Transport Layer Security, « Sécurité de la couche de transport », pour le commerce électronique (qui peut également fournir un service de confidentialité par chiffrement)
- ❖ Kerberos, standard utilisé par Windows et Linux pour se connecter sur une machine

Une authentification simple : est une procédure d'authentification qui requiert un seul élément ou «facteur» d'authentification valide pour permettre l'accès à une ressource.

Une authentification forte : est une procédure d'authentification qui requiert au moins deux éléments ou « facteurs » d'authentification valides pour permettre l'accès à une ressource. Ex. carte bancaire (1. être en possession de la carte; 2.connaître le PIN)

Une authentification mutuelle : impose une double authentification entre les deux entités.

L'authentification peut inclure une phase d'identification, au cours de laquelle l'entité indique son identité.

Cependant, cela n'est pas obligatoire ; il est en effet possible d'avoir des entités munies de droits d'accès mais restant anonymes.

L'identification : permet donc de *connaitre l'identité d'une* entité alors que l'authentification permet de *vérifier cette* identité

13) Intégrité des données :

L'intégrité des données consiste à vérifier qu'elles n'ont pas été altérées accidentellement ou frauduleusement au cours de leur transmission ou de leur stockage. Ce principe regroupe un ensemble de fonctionnalités mises en œuvre afin de s'assurer de leur intégrité, comme les fonctions de hachage

14) Un mécanisme de non-répudation :

Permet d'empêcher à une personne de nier le fait qu'elle a effectué une opération (exemple : envoi d'un message, passage d'une commande).

Pour assurer la non-répudiation d'un message, on peut, par exemple, utiliser la signature électronique.

15) La confidentialité :

est la propriété qui assure qu'une information ne peut être lue que par des entités habilitées (selon des contraintes précises)

Le chiffrement (cryptage) : est le procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

On distingue deux familles de systèmes de chiffrement :

- Chiffrement symétrique ou à clé privé.
- Chiffrement asymétrique ou à clé publique (en réalité utilisant une paire de clés)