La Sécurité Informatique
En Utilisant Windows 7 et Office 2010

TABLE DES MATIERES

1 LES CONCEPTS DE LA SECURITE

Avec le développement de la science et de la technologie, ainsi que le développement des différents moyens de stockages d`informations et l'échange d'informations selon différentes méthodes ou ce que l'on appelle **« transfert des données via le réseau d`un site à un autre »** à changer le regard porté sur l'importance de la sécurité de ces informations et données.

La sécurité de l`information est une science qui offre la protection des informations contre toutes menaces de vol ou de modification et cela en proposant des outils et des moyens pour protéger les informations contre tous les dangers internes ou externes ainsi que l`application de normes et de procédures de communication pour empêcher l`accès des personnes non autorisées aux données, et assurer leurs originalités et la validité de ces communications.

1.1 Les menaces de données

1.1.1 Distinguer entre les données et les informations

- **Les données** : cela peut être des caractères, des mots, des chiffres, des codes, des images, des sons qui ne sont pas encore traités, le but est de récolter ces données pour les traiter. On peut dire que les données sont des informations non traitées.
- **Les informations** : ce sont des données après le traitement, elles auront un sens pour la personne qui les réceptionne.

Pour faire la différence entre les données et les informations, prenons cet exemple : les mots suivants **« ALI, 920,92 »** sont des données, par contre lors de leurs interprétations pour : un étudiant prénommé « **ALI** », l`ensemble de ses notes est « **920** », et sa moyenne est « **92** », deviennent des informations.

Il est à signaler qu`au moment de l`interprétation des données différemment, cela implique aussi différentes informations.

1.1.2 La cybercriminalité

Tout travail illégal en utilisant l`internet ou l`ordinateur, par exemple : le vol de l`identité d`une personne, l`ingénierie sociale, le hack sécuritaire, cracker la protection des programmes, vols de détails de carte de crédits via l`internet.

La cybercriminalité inclut toute violation contre des individus ou des groupes par motif criminel, ou le non-respect de l`image de la victime d`une manière verbale et corporal. Tout ça en utilisant des moyens de communication récents comme l`internet, le salon de chat, courrier électronique, ou les associations etc...

1.1.3 La différence entre le piratage et le piratage éthique

- Le piratage utilise la créativité, l`expérience informatique pour accéder au système de l`ordinateur sans autorisation, dans le but de falsifier les données et les programmes existants dans l`ordinateur pour des fins d`espionnage ou de vols d`argent. Le pirate peut aussi utiliser les ressources de l`ordinateur ou se contente de prouver qu`il est capable d`accéder à la machine.

- Le piratage éthique est utilisé pour pirater le système sécuritaire de l`ordinateur, autres, mais pour protéger le système de l`ordinateur en cherchant les points faibles et failles sur le réseau dont le pirate peut en profiter. Le pirate éthique essaye de franchir tous les obstacles des systèmes de protection qui l`opposent dans l`objectif d`accéder à une information non autorisée, il y a des cas ou le pirate tente de paralyser le système dans le but de faire barrage aux utilisateurs pour ne pas accéder toujours au système ou aux services. Cette opération de piratage éthique prend fin en présentant un rapport détaillé sur le plan de sécurité qu`offre cette organisation, elle peut encore apporter des améliorations pour éviter les risques qui touchent l`organisation durant les tentatives des pirates non-éthiques. déclaré par une autorisation du propriétaire mais pas pour désactiver le service ou

- Craquer le mot de passe est la rédemption et la découverte de mots de passe soit à partir des données stockées, ou bien celles transférées par le système de l`ordinateur. cet ordre se fait soit manuellement en craquant le mot de passe ou en utilisant les programmes spéciaux.
- Craquer les programmes de protection, cela en supprimant certains avantages non désirés comme par exemple : les droits de publication, les codes confidentiels, les dates de consultation, le code PIN.

1.1.4 Les menaces sur les données par force majeure

Les forces majeures sont les événements imprévus que la société ne peut pas prévoir, comme les incendies, les inondations, les guerres, les séismes, ceci pourront détruire toutes les données des individus et de toutes les sociétés.

1.1.5 Les menaces des données par des individus

Le risque des individus n`est pas moins que les forces majeures, la probabilité de vol des données et leurs utilisations à des fins personnelles ou monétiques est une probabilité relative élevée si vous ne prenez pas les prérogatives de protection nécessaires, parmi les individus qui accèdent aux données, on trouve :

- **Les employées**: Les employées peuvent voler les données de l`entreprise, comme les informations sur un nouveau produit de l'entreprise soit pour leurs compte personnel ou pour le compte d'un individu externe.

- **Les fournisseurs de services**: les employées du fournisseur de services peuvent consulter les données d'une manière volontaire ou non-volontaire, comme ils peuvent aussi détruire ou voler les données de valeur de la société car c`est eux qui font le traitement des données de la société sur le matériel du serveur.
- **Les individus de l`extérieur**: comme les pirates, ils peuvent accéder au système de l`ordinateur pour voler ou supprimer les données.

Exercice (1-1)

Choisir la bonne réponse parmi les quatre propositions disponibles: (**Voir l'annexe des réponses aux questions p93**).

1. Qu`appelle-on l`activité illégale en utilisant l`internet ?
   a. La cybercriminalité
   b. Site de la criminalité
   c. Le crime physique
   d. Le crime virtuel

2. Parmi ces exemples, lequel est un crime de l`internet ?
   a. Le piratage éthique
   b. La déchirure
   c. Le phishing
   d. Le pare feu

3. La définition du piratage éthique est :
   a. Espionnage à travers le réseau de communication sans fil
   b. L`accès autorisé au système
   c. L`accès non autorisé au système
   d. Espionnage à travers le réseau de communication filaire

4. Parmi ces propositions, laquelle n'est pas une force majeure et qui est une menace pour les données ?
   a. Les fournisseurs de services
   b. Les incendies
   c. Les inondations
   d. Le séisme

5. Que veut dire, cracker les mots de passe ?
   a. Faire entrer le mot de passe incorrect plusieurs fois
   b. Connaitre le mot de passe
   c. Voler les détails personnels d`une personne via internet
   d. Modifier le mot de passe d`une manière périodique

6. Parmi ces propositions laquelle n'est pas une menace pour données ?
   a. Les pirates
   b. Fournisseurs de service
   c. Les certificats numériques
   d. Les employées

7. Qu`appelle-on les informations?
   a. Les donnes traitées
   b. Les sons et les textes
   c. les chiffres non traités
   d. les données non traitées

8. Qu`appelle-on le piratage de système de sécurité de l`ordinateur, déclaré par une autorisation du propriétaire ?
   a. Le piratage
   b. Cracker la protection des programmes
   c. Le vol d'identité
   d. Le piratage éthique