# TD n° 3: Protection et mécanismes de sécurité

**Exercice 1 :**

1. Quelles sont les trois stratégies de base qui peuvent être utilisées comme mécanismes de sécurité ?

2. Pour chacune des stratégies de la question précédente, donner un exemple d'une situation dans laquelle l'énoncé suivant est correcte :

a) La 1ére stratégie est plus importante que les autres.

b) La 2éme stratégie est plus importante que les autres.

c) La 3éme stratégie est plus importante que les autres.

**Exercice 2 :**

Considérons les actifs suivants pour une société d'agence de voyage :

- Un serveur web qui fournit un service de réservations de voyages sur Internet.
- Un ordinateur portable du service commercial contenant les catalogues des clients.

1. Dresser une liste des menaces pour chaque actif.

2. Faire une évaluation des vulnérabilités des actifs pour les cas suivants :

a) Le serveur web est indépendant de son milieu (aucun pare-feu ou anti-virus, le système n'est pas mis à jour).

b) l'ordinateur portable se trouve dans un bureau à accès limité et est protégé par un anti-virus et par un pare-feu.

c) Le serveur web est protégé par un pare-feu, le système d'exploitation est sécurisé par un anti-virus mais l'agence ne sait pas s'il est à jour ou non.

d) L'ordinateur portable est protégé par un anti-virus et un pare-feu mais il est partagé par plusieurs employés et peut même être déplacé à l'extérieur de l'agence.

3. La valorisation des actifs de l'agence est définit tel que suit : ***(CA = Chiffre d'Affaires)***

***0*** *→ Aucune conséquences*
***1*** *→ perte < un jour de CA*
***2*** *→ perte < une semaine de CA*
***3*** *→ perte < un mois de CA*
***4*** *→ perte > un mois de CA.*

En vous basant sur ces critères de valorisation, donner la valeur de chaque actif selon le modèle de sécurité CIA, en sachant que pour :

- Le serveur web : Une perte d'informations confidentielles peut être gérée moyennement, mais des problèmes de modification ou d'interruption du serveur peuvent avoir des conséquences catastrophiques.
- L'ordinateur portable : le fichier des clients présent sur l'ordinateur portable est l'élément capital de l'agence, sa divulgation conduirait à des pertes de presque un mois de CA. Ce fichier est sauvegardé sur un support externe, donc une modification de ce fichier ou une indisponibilité de l'ordinateur peuvent être supporté pendant une journée.

4. En sachant que la vraisemblance d'une menace correspond à la probabilité d'occurrence de cette menace et en quantifiant les valeurs de vraisemblance à 6 niveaux (0 : aucun, 1 : bas…, 5 : haut). Donner une estimation de la vraisemblance pour les vulnérabilités de chaque cas de la question 2 et calculer la valeur du risque correspondant.

5. Que remarquez-vous entre la valorisation de l'actif et les vulnérabilités/menaces.

**Exercice 3 :**

1. Soit les sujets : Amine, Mohamed et Khadija. Soit les objets (de type fichier) : fichier1, fichier2 et fichier3 appartenant respectivement aux 3 sujets.

a) En considérant les propriétés suivantes, représenter la matrice d'accès :

- Amine peut lire fichier2.
- Mohamed et Khadija peuvent lire fichier1.
- Khadija peut écrire sur le fichier2.
- Chaque propriétaire peut exécuter les fichiers qui lui appartiennent

b) Khadija donne à Amine le droit d'exécuter le fichier3, Amine retire le droit de lire à Mohamed sur ses fichiers. Représenter la nouvelle matrice d'accès.

2. Un utilisateur souhaite utiliser un cybercafé pour se connecter à son compte personnel, mais il soupçonne que l'ordinateur est infecté par des keyloggers. En supposant qu'il a une fenêtre de navigateur Web et une fenêtre d'édition de texte ouverts en même temps.

a) Décrire un schéma qui lui permettra de protéger ses données sensibles contre les logiciels malveillants concernés.

b) Décrire deux mécanismes de sécurité pour la défense contre les keyloggers.

**Exercice 4 :**

1. Une menace ciblant les clients de la banque BNP Paribas a été détectée. Elle se présente sous la forme d'un message intitulé « Votre compte », envoyé en apparence par la banque (L'équipe Internet BNP Paribas <no-replay@bnp-paribas.dz>) :

**********

***Cher client***

***Nous avons récemment déterminé que plusieurs ordinateurs sont connectés à votre compte bancaire en ligne, de plus, plusieurs saisies de mots de passe incorrectes ont été enregistrés lors des tentatives de connexions.***

***A cet effet, nous somme obligés de suspendre votre compte indéfiniment, car il se peut qu'il ait été utilisé à des fins frauduleuses. Nous vous remercions de votre coopération et nous nous excusons pour le désagrément causé.***

***Afin de vérifier vos informations et réactiver votre compte, cliquer sur le lien suivant :***

***>>>>>Cliquer ici pour vérifier votre compte bancaire en ligne<<<<<***

***NB : Ce message vous est adressé automatiquement. Merci de ne pas y répondre.***

**********

a) Donner le nom de cette infection informatique en français puis en anglais.

b) Quel mécanisme de sécurité peut être utilisé pour se protéger contre cette infection ?

c) Expliquer la meilleure méthode pour une prévention contre cette infection ?

2. Le message est accompagné d'un fichier joint bnp.zip qui contient un fichier bnp.exe qui permet à l'expéditeur de prendre le contrôle de la machine infectée et de récupérer les données bancaires et autres données sensibles à l'insu de la victime, lors de transactions légitimes :

a) Donner le nom de cette infection informatique en français puis en anglais.

b) Justifier la réponse de la question a.

c) Comment se protéger contre cette infection ?

d) Expliquer la meilleure méthode pour une prévention contre cette infection ?

e) Expliquer l'intérêt de cette menace associant les deux infections informatiques citées auparavant.