

Date : 14/12/2021 Session : 2021-2022

Diplôme / filière / niveau : Master 2 TI

UE : Sécurité des systèmes
d'information

Épreuve : partie 2 EBios

Note : (de 0 à 20)

Appréciation du correcteur :

Signature du/des correcteur(s) :

Partie EBios

2) source de Menace
Menace

Vulnérabilité

Bien support

Bien essentiel

Besoin de sécurité

Impact

4/1. Eviter le risque : supprimer le bien support
associé au risque

2. Réduire le risque : Agir sur les vulnérabilités
du bien support

3. Prendre le risque : Ne rien faire, estimer que
le risque est minime

5. Transférer le risque : Déléguer le risque à
une tierce

Cette décision s'appelle l'objectif de sécurité.

Si votre composition
comporte plusieurs
feuilles

numérotez les/.....

5) On valide la décision avec le maître d'ouvrage.

Si l'acceptation des risques n'est pas possible, on peut essayer de faire des compromis sur certain risque.

En l'état l'acceptation du risque n'est pas possible car les risque résiduel de R4 sont trop important.

4

Question n°1 (4 points)

Pour la liste des libellés ci-dessous :

- Veuillez dire s'il s'agit d'une menace ou d'une vulnérabilité
- Veuillez donner des vulnérabilités associées s'il s'agit d'une menace.
- Veuillez donner des menaces associées s'il s'agit d'une vulnérabilité.

Vulnérabilité ou Menace ?	V ou M	Catégorie de bien support concerné	Indiquez une liste de vulnérabilités exploitables par la menace ou des menaces capables d'exploiter la vulnérabilité
Données non effacées des serveurs du prestataire et rendues accessibles	M	Matériel	Manque de chiffrement Absence de vérification de suppression
Espionnage	M	Personnel	Absence de contrôle à l'entrée du bâtiment Absence de badge d'accès
Transfert du mot de passe en clair	M	Réseau	Absence de chiffrement point à point Absence de chiffrement des mots de passe sauvegardés
Politique de mot de passe faible	V		Attaque par brute force Mot de passe évident à deviner
Faible loyauté	V	Personnel	Divulcation d'informations à des concurrents. Départ de l'entreprise
Action d'un aimant sur un disque dur	M	Matériel	Disque dur non protégé Disque dur accessible par tout le monde
Datacenter mal protégé contre les catastrophes naturelles	V	Locaux	Incendie Séisme
Sujet à la dissipation	M		

Question n°2 (2 points)

Veillez rappeler quelles sont les sept composantes d'un risque et retrouvez ces sept composantes dans le risque rédigé suivant :

Risque

Les administrateurs du site de vente en ligne de l'entreprise commettent une erreur de configuration due à un manque de formation. Ceci entraîne une indisponibilité du site qui est aggravée par un manque d'organisation dans le processus de sauvegarde / restauration. L'impact est une perte financière de 10 000 € à chaque heure d'indisponibilité.

Vous pouvez présenter les résultats sous la forme d'un tableau de ce type :

Composante 1	Source de Menace : Administrateurs du site
Composante 2	Menace : Erreur de configuration
Composante 3	Vulnérabilité : Manque de formation
Composante 4	Bien support : Site internet
Composante 5	Bien essentiel : processus de sauvegarde restauration
Composante 6	Besoin de sécurité : Améliorer l'organisation dans le processus de sauvegarde
Composante 7	Impact : perte financière de 10000€ à chaque heure d'indisponibilité

Question n°3 – 8 points

Dans cette question, les libellés des objets manipulés ne sont pas utiles à la réalisation de l'exercice. Votre travail consiste ici, à l'aide des tableaux fournis, à identifier et estimer les risques.

Voici quatre scénarios de menace identifiés avec leur vraisemblance :

En utilisant les tableaux précédents, veuillez identifier et estimer les risques.

- Si les vulnérabilités V1 et V3 sont présentes, alors la source de risque SR1 pourra utiliser M9 (vraisemblance 1)

Risque 1 :

$SR1 \rightarrow M9 \rightarrow V1, V3 \rightarrow \underbrace{S2, S4}_{\text{très complexe}} \rightarrow \underbrace{E5, E2}_{\text{valeur du bien} = 3}$

Vraisemblance 1 \rightarrow Risque = 2

- Si les vulnérabilités V2 et V5 sont présentes, alors la source de risque SR2 pourra utiliser M20 (vraisemblance 3)

Risque 2 :

$SR2 \rightarrow M20 \rightarrow V2, V5 \rightarrow \underbrace{S1, S2}_{\text{moyen}} \rightarrow \underbrace{E2, E5}_{VB = 3}$

Vraisemblance 3 \rightarrow Risque = 5

- Si les vulnérabilités V4 ou V5 sont présentes, alors la source de risque SR3 pourra utiliser la menace M14 (vraisemblance 2)

Risque 3 :

$SR3 \rightarrow M14 \rightarrow V4 \text{ ou } V5 \rightarrow \underbrace{S3, S2}_{\text{facile}} \rightarrow \underbrace{E1, E3, E5}_{VB = 4}$

Vraisemblance 2 \rightarrow Risque = 6

- Si les vulnérabilités (V1 et V6) ou (V2 et V5) sont présentes, alors la source de risque SR4 pourra utiliser la menace M13 (vraisemblance 2)

Risque 4 :

$SR4 \rightarrow M13 \rightarrow \underbrace{V1, V6}_1 \text{ ou } \underbrace{V2, V5}_2 \rightarrow \underbrace{S2, S5, S1}_{\text{VB} = 5}$

$\rightarrow \underbrace{E2, E5, E4}_{VB = 4}$

Vraisemblance 2 \rightarrow Risque = 5

Question n°4 (3 points)

Nous passons à la phase de traitement du risque.

Les 4 risques identifiés et estimés à la question 3 sont présentés au maître d'ouvrage par le maître d'œuvre de l'étude de sécurité. Notre maître d'ouvrage doit décider de la façon dont va être engagé le traitement de ce risque.

Comment s'appelle cette décision ?

Ce type de décision peut appartenir à quatre grandes catégories. Veuillez lister ces catégories et expliquer en quoi consiste chacune d'entre-elles.

Question n°5 (3 points)

Pour les 4 risques, on décide de mettre en place 10 mesures de sécurité. Le tableau suivant donne la couverture des risques par les mesures. Chaque case du tableau représente une estimation de l'abaissement du risque si la mesure est mise en place. Les risques de valeur inférieur ou égal à 2 sont considérés comme acceptables.

Calculez le risque résiduel.

	Risque initial	Risque résiduel	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
R1	2	0,5		0,5	0,5				0,5			
R2	5	2	1	0,5	0,5		0,5					0,5
R3	6	1	1	0,5	0,5			1		1	1	
R4	5	3,5	0,5			0,5	0,5					

L'acceptation des risques est-elle possible en l'état ? Sinon que peut-on faire ? Avec qui validez-vous cette décision ?

— FIN —