UNIVERSITÉ DE PAU ET DES PAYS DE L'ADOUR

UFR Sciences et Techniques Pau

Date : 14/12 Session : 1ere Th

Diplôme / filière / niveau : M2 TI

UE : Partie7 EBios

Épreuve :

Note : ..... (de 0 à 20)

Appréciation du correcteur :

Signature du/des correcteur(s) :

Si votre composition comporte plusieurs feuilles

numérotez les ...../.....

1

11

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	Serveurs	Trouver des données confidentielles accès à des factures, commandes, fiche de paies etc
Espionnage	M	Confidentialité	Réseau peu protégé Écoutes
Transfert du mot de passe en clair	~~V~~ M	confidentialité	Attaque, vol de données accès aux comptes personnels
Politique de mot de passe faible	V	confidentialité	Piratage de mot de passe
Faible loyauté	V	personnel	La concurrence lui achète des informations Espionnage industriel
Action d'un aimant sur un disque dur	V	Hardware	Vol d'infos Disque dur Corrompu
Datacenter mal protégé contre les catastrophes naturelles	V	Hardware	Tsunami, tremblement de terre
Sujet à la dissipation	V	Personnel	Donner des infos à la concurrence Aucun respect pour l'entreprise

Question n°2 (2 points)

Veuillez 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 risque : manque de formations, erreurs
Composante 2	Menace, mode opératoire : indisponibilité du site
Composante 3	Vulnérabilité : erreur de configurat°
Composante 4	Bien support : site de vente en ligne
Composante 5	Bien essentiel : formations
Composante 6	Besoins de sécurité : manque d'organisation processus sauvegarde/restauration
Composante 7	Impact, conséquence : perte financière 10 000€/heure.

M1

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 : Si V1 et V3 sont présentes, S2 et S4 sont touchés et touchent encore E5 et E2. V1 touche S2 et est une vulnérabilité complexe. V3 => S4, vulnérabilité moyenne
Il est inutile d'utiliser M9 si il y a que V1, mais couplé à V3, on touche directement à la disponibilité et intégrité et sécurité. On peut alors utiliser M9

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

Risque 2 : Lorsque ces deux vulnérabilités sont présentes, on a un gros souci sur le bien essentiel E2 car D = 3 I = 4 et C = 3
On peut utiliser le code M20 lorsque la confidentialité est touché

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

Risque 3 : On peut utiliser la menace M14 car :
V4 → S3 → E1 : D,I,C = 1,1,4
E3 : D,I,C = 2-2-0
V5 → S2 → E5 = D,I,C = 0,0,1
La V4 menace grandement la confidentialité, on peut utiliser M14

- 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 : Si V1 et V6, il n'y a pas besoin de utiliser M13.
V1 → S2 → E5 → 0,0,1
V6 → S5 → E4 → 1,1,0
Si V2 et V5, on peut utiliser M13 car elle atteint fortement Det I
V2 → S1 → E2 → 3,4,3
V5 → S2 → E5 → 0,0,1

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				**0,5**	**0.5**				**0.5**			
R2			**1**	**0.5**	**0.5**		**0.5**					**0,5**
R3			**1**	**0.5**	**0.5**			**1**		**1**	**1**	
R4			**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 –