13

UNIVERSITÉ DE PAU ET DES PAYS DE L'ADOUR

UFR Sciences et Techniques Pau

Date : 14/12/2024 Session : 1

Diplôme / filière / niveau : M2 TI

UE : Sécurité des Systèmes d'Information

Épreuve : EXAM

Note : ..... (de 0 à 20)

Appréciation du correcteur : .....

Signature du/des correcteur(s) :

Partie EBIOS (Frédéric Kurtzan)

Question 4 :

Cette décision s'apelle l'appréciation des risques

les 4 grandes catégorie sont les suivantes :

- Eviter le risque : tout mettre en oeuvre pour empêcher que le risque se produise
- Réduire le risque : mettre des choses en oeuvre permettant de réduire les conséquence du risque
- Prendre le risque : estimer que le risque est peu probable et que les conséquence sont moindre et donc ne pas le prendre en compte
- Transférer le risque :

Si votre composition comporte plusieurs feuilles

numérotez les ...../.....

13

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	V	MAT	Menace : - Revente des infos personnelles - Intrusion après récupération de mot de passe
Espionnage	M	PERS	Vulnérabilités : - personne naïve - personnel non loyale - manque de formation du personnel
Transfert du mot de passe en clair	V	CAN	Menaces : - quelqu'un intercepte le mot de passe - via ce mot de passe quelqu'un accède au compte et récupère des données personnelles
Politique de mot de passe faible	V	PER	Menaces : - Quelqu'un peu le découvrir avec une attaque Brute de force
Faible loyauté	V	PER	Menaces : - Personnes travaille pour la concurrence - Détournement de fond - Sabotage
Action d'un aimant sur un disque dur	M	MAT	Vulnérabilités : - Coeur non sécurisé
Datacenter mal protégé contre les catastrophes naturelles	V	LOC	Menaces : - Incendie - Tornade - Inondation
Sujet à la dissipation	V	PERS	Vulnérabilités : - Envie de manipulation

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 Menace	Administrateurs
Composante 2 Menace (mode opératoire)	Erreur de configuration (manipulation)
Composante 3 Vulnérabilités	Manque de Formation Manque d'organisation dans le processus de sauvegarde / restauration
Composante 4 Biens supports	- Administrateurs - Site de vente
Composante 5 Biens essentiels	- Processus de sauvegarde
Composante 6 Besoins de sécurité	- Disponibilité - Intégrité
Composante 7 Impact	- Perte d'argent considérable - Perte de client régulier

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 :

SH1 → M9 (VR=1, D) → V1 et V3 (1 → faible) → S2, S4 → E5, E2 (3)

R=2

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

Risque 2 :

SH2 → M20 (VR=3, C) → V2 et V5 (2 → Moyen) → S1, S2 → E2, E5 (3)

R=5

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

Risque 3 :

SH3 → M14 (VR=2, C) → V4 ou V5 (3 → Facile) → S2, S2 → E1, E5 (4)

R=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 :

SH4 → M13 (VR=2, D,I) → (V1 et V6) ou (V2 et V5) (1 et 2 → 2 → Moyen) → S2, S1, S5 → E2, E4, E5 (4)

R=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**			
R2	5		**1**	**0.5**	**0.5**		**0.5**					**0,5**
R3	6		**1**	**0.5**	**0.5**			**1**		**1**	**1**	
R4	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 –