

Date : 14 déc 2021 Session : 2021-2022

Diplôme / filière / niveau : Master 2

Technologies de l'Internet

UE : SS I - Partie 2

EBIOS

Épreuve : Examen

Note : (de 0 à 20)

Appréciation du correcteur :

Signature du/des correcteur(s) :

Question 4:

Une fois les risques étudiés et évalués vient la phase de traitement.

Il y a quatre grandes décisions:

- Éviter le risque
- Réduire le risque (on prend des mesures)
- Prendre le risque (faible indice, on ne fait rien pour)
- Transférer le risque (on le confie à un tiers).

Question 5:

cf sujet

Il reste encore un risque important R4. Il faut voir quelles mesures peuvent être prises avec les décideurs.

Questions 1 à 3:

cf sujet

Si votre composition
comporte plusieurs
feuilles

numérotez les/.....

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	SYSMAT	.faible politique de confidentialité
Espionnage	M	SYSMAT	.poste de travail sans mot de passe. .poste sans antivirus
Transfert du mot de passe en clair	M	SYSRES	.faible connaissance en sécurité informatique .Pas de chiffrement
Politique de mot de passe faible	✓	SYSLOG	.Vol de données .Usurpation d'identité
Faible loyauté	✓	ORGPERS	.Espionnage industriel
Action d'un aimant sur un disque dur	M ✓	SYSMAT	.Corruption de données
Datacenter mal protégé contre les catastrophes naturelles	✓	ORGLOC	.Incendie .Perte de courant
Sujet à la dissipation	✓	ORGPAP	.Perte de données

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 menace	indisponibilité du site
Composante 2 source de menace	administrateurs du site
Composante 3 vulnérabilité	personnel mal formé manque d'organisation
Composante 4 bien support	serveur web
Composante 5 bien essentiel	site de vente
Composante 6 besoin de sécurité	sauvegarde / restauration
Composante 7 impact	Pertes financières (10 000 €/h)

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 : ~~V1~~ ^{V3} :
Le dépassement des limites du logiciel implique une question de disponibilité. Sachant que ~~V1~~ n'en implique pas, son impact est minime.

indice de vraisemblance : 1

indice du risque : 2

indice de valeur : 3

=>

indice de facilité : 2

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

Risque 2 : L'espionnage indique un besoin de confidentialité.

indice de vraisemblance : 3

indice de valeur : 3

=>

indice du risque : 5 Δ

indice de facilité : 2

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

Risque 3 : L'écoute passive donne un besoin de confidentialité

indice de vraisemblance : 2

indice de valeur : 4 ou 1

indice de facilité : ~~3~~
1 ou 3

=>

indice du risque (V4) : ~~4~~ 4

(V5) : 3

indice du risque : 4 Δ

- 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 : Une attaque donne des besoins de disponibilité et d'intégrité

indice de vraisemblance : 2

indice de valeur : 1 ou 4

indice de facilité : 1 ou 2

=>

indice du risque (V1 & V6) : 1

(V2 & V5) : 5

indice du risque : 5 Δ

On donne le tableau de **croisement des biens essentiels (E1, ..., E5) et biens supports (S1, ..., S5)**.

	E1	E2	E3	E4	E5
S1		x			
S2					x
S3	x		x		
S4		x			
S5				x	

Voici le tableau de **synthèse des besoins de sécurité**.

	Disponibilité	Intégrité	Confidentialité
E1	1	1	4
E2	3	4	3
E3	2	2	0
E4	1	1	0
E5	0	0	1

Les menaces génériques suivantes ont été sélectionnées dans la base de connaissance de la méthode.

Support	Type	Code	Libellé	D	I	C
LOG	DEP	M9	Dépassement des limites d'un logiciel	x		
RSX	USG	M13	Attaque du milieu sur un canal informatique ou de téléphonie	x	x	
RSX	ESP	M14	Écoute passive d'un canal informatique ou de téléphonie			x
PER	ESP	M20	Espionnage d'une personne à distance			x

Voici le tableau des vulnérabilités et les biens supports concernés. Les niveaux de vulnérabilités sont indiqués avec l'échelle suivante représentant la complexité d'utilisation :

3 : Facile à exploiter

2 : Moyen

1 : Complexe

	V1	V2	V3	V4	V5	V6
S1		2				
S2	1				3	
S3				1		
S4			2			
S5						3

Vous utiliserez ce tableau pour calculer la valeur du risque.

Vraisemblance de la menace		Improbable : 1			Probable : 2			Certain : 3		
Facilité d'exploitation		C	M	F	C	M	F	C	M	F
Valeur des biens	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7

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 inférieure 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	4	—	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 —