Université 8 Mai 45 Guelma
Département d'Informatique
Sécurité des SI
ISIL

Série 2 : Analyse des risques

Exercice 1.

Soit les risques suivants :

- L'endommagement des dispositifs matériels: câblage et dispositif de sécurité engendre la possibilité de non fonctionnement ou de fonctionnement incorrect d'un équipement.
- L'altération du media support de logiciel, ou de paramètres de processus peut engendrer la modification des échanges avec cet équipement.

1- Designer les actifs primaires et secondaires (supports).

2- Identifier les composants de ces risques (biens essentiels, sources des menaces, impacts, critères de sécurité menacés et les menaces.

3- Soit l'actif *paramètres de processus* (3,5,2). La vraisemblance du risque pouvant menacé cet actif est estimée à 2, calculer le niveau du risque.

Exercice 2.

Faire une analyse des risques d'une direction d'entreprise qui utilise un réseau où les partages sont activés par défaut pour toute les machines du réseau afin de pouvoir récupérer les scans ou les fax reçus. L'imprimante permet de stocker des documents. L'imprimante peut être contrôlée à distance sur Internet.

- Etudier les risques de failles de sécurité informatique qui pourrait avoir un impact sur cette entreprise.

Exercice 3

I- Considérons un site web qui fournit un service de réservations de vol sur Internet. Soit l'actif serveur web (1, 5, 5) qui héberge ce site tel qu'aucun moyen de sécurité n'est adopté. La probabilité d'occurrence d'une menace au serveur (POM) est estimée à 3 et la Facilité d'Exploitation de la vulnérabilité (FEV) est estimée à 3 également.

1. Quel est le type de l'actif serveur Web
2. Calculer la vraisemblance d'une menace sur cet actif
3. Calculer le niveau de risque

– Les utilisateurs ne peuvent pas accéder au site. Les journaux système indiquent que le serveur qui Web fonctionne lentement en raison du nombre élevé des fausses requêtes qu'il reçoit.

4. De quelle technique d'attaque s'agit-il ?
5. En fonction du niveau du risque Quel type de traitement du risque peut-on adopter (A,D,T,E)?

L'administrateur du site a envisagé de procéder au traitement de transfert du risque et la responsabilité de la réponse à ce risque à l'administrateur du serveur web.

6. La procédure de transfert de risque permet d'éviter quelle conséquence ?
7. Proposer 2 contre-mesures (solutions) pour renforcer la sécurité du serveur Web.

Université 8 Mai 45 Guelma
Département d'Informatique
Sécurité des SI
ISIL

Série 2 : Analyse des risques

Exercice 3

Type de l'actif : Actif primaire

1. Calculer la vraisemblance d'une menace sur cet actif

La vraissemblance=POM+FEV-1

=3+3-1=5

2. Calculer le niveau de risque

Niveau de risque= Max (C, I, D)* vraisemblance

=Max (1, 5, 5)*5=25

– Les utilisateurs ne peuvent pas accéder au site. Les journaux système indiquent que le serveur qui Web fonctionne lentement en raison du nombre élevé des fausses requêtes qu'il reçoit.

3. De quelle technique d'attaque s'agit-il ?

C'est une attaque de type Denis de service (DoS)

4. En fonction du niveau du risque Quel type de traitement du risque peut-on adopter (A, D, T, E)?

Pour les niveaux de risque compris entre 20 à 25 : traitement obligatoire => A, D, T ou E

Dans ce cas on ne peut pas adopter le traitement A accepter et Eviter parce que l'acceptation du risque ne signifie qu'aucune action à prévoir et pour le traitement Eviter on ne peut pas supprimer l'Actif ou Arrêter le service !

Alors le traitement choisi sera : Transférer (Déplacer la responsabilité du risque sur un tiers) ou D diminuer (Choisir une mesure dans la norme 27001)

L'administrateur du site a envisagé de procéder au traitement de transfert du risque et la *responsabilité* de la réponse à ce *risque* à l'administrateur du serveur web.

5. La procédure de transfert de risque permet d'éviter quelle conséquence ?

- « transfert des risques » signifie les manières d'éviter d'avoir à payer pour les erreurs associées aux activités et produits contrôlés par des tiers (partenaires d'affaires, sous-traitants, fournisseurs, etc.). L'idée est de faire en sorte que la partie la mieux équipée pour contrôler les risques assume la responsabilité. **Le but est également de s'assurer que ces tiers aient la capacité financière de payer**.

6. Proposer 2 contre-mesures (solutions) pour renforcer la sécurité du serveur Web.

a. Les contrôles de connexion empêchent la surcharge en ressources du serveur en limitant les taux de connexion, les taux de requêtes, et autres variables pour chaque utilisateur des bases de données.

b. Le contrôle d'accès des requêtes, pour détecter toutes requêtes non autorisées pouvant créer un déni de service.

c. Le contrôle du temps de réponse -response timing– les attaques de déni de service des bases de données visant à surcharger le serveur en ressources provoquent des réponses de bases de données différées.

Université 8 Mai 45 Guelma
Département d'Informatique
Sécurité des SI
ISIL

Série 2 : Analyse des risques

Exercice 2

Actifs	Type de l'actif	Menace	Critère de sécurité menacé	Impact	Solution
Imprimante 0,5	Secondaire 0,5	-Coupure électrique, 1,5	Disponibilité 0,5	-Arrêt de l'activité. 0,5	-Effectuer des mises à jour du pilote 1
		-Panne du serveur -Attaque techniques ou virale.		-Perte des données,	-Contrôle d'accès adéquat -Renforcement de la sécurité au niveau du serveur. -Utilisation de firewall
Documents 0,5	Primaire 0,5	-Usurpation des droits d'accès, -Manque de protection réseau, 1,5 -Absence de sensibilisation des usagers -Panne du serveur	Confidentialité Disponibilité Intégrité 1,5	-Perte des données, -Perte financière. -Perte de confiance des clients. 1,5	-Cryptage efficace -Contrôle d'accès sophistiqué -Duplication des données -Renforcement de la sécurité au niveau du serveur et du reseau 1

Exercice 1 :

1-

Actifs primaires: /

Actifs secondaires : câblage et dispositif de sécurité, media support de logiciel, paramètres de processus.

Risque 1 :

1. Bien essentiel : dispositifs matériels (câblage et dispositif de sécurité)
2. Source de menace : humaine interne accidentelle/externe volontaire
3. Impact : la possibilité de non fonctionnement ou de fonctionnement incorrect d'un équipement, perte financière, arrêt de l'activité.
4. Critère de sécurité menacé : disponibilité
5. Menaces : l'eau, la chaleur, changement climatique…etc.

Risque 2 :

1. Bien essentiel : media support de logiciel, ou de paramètres de processus
2. Source de menace : humaine interne involontaire
3. Impact : la modification des échanges avec cet équipement, arrêt de l'activité, perte financière (maintenance).
4. Critère de sécurité menacé : intégrité
5. Menaces : manque de protection du logiciel, absence de sensibilisation des usagers.

3- Soit l'actif *paramètres de processus* (3,5,2). La vraisemblance du risque pouvant menacé cet actif est estimée à 2, calculer le niveau du risque.

Risque =MAX(C, I, D)*vraisemblance=5*2=10