Université 08 Mai 45 – Guelma
Département informatique
3ème année Licence (SI, ISIL)
Module : Sécurité Informatique

Correction Travaux Dirigés [série n°1]

Question 1 :

Les principaux objectifs de sécurité informatique sont de réaliser :

- la confidentialité,
- l'intégrité,
- la disponibilité des données et des services du système.

Diverses mesures de sécurité permettent de les atteindre. Parmi elles nous pouvons citer :

- le contrôle d'accès,
- le chiffrement de données,
- la gestion des incidents, des erreurs, des dysfonctionnements, des intrusions,…

Question 2 :

Capacité d'un système à	Objectif de sécurité	Moyens de sécurité
Pouvoir être utilisé	• disponibilité	• Dimensionnement • Redondance • Procédure d'exploitation et de sauvegarde
Exécuter des actions	• Sûreté de fonctionnement • Fiabilité • Durabilité • Continuité • Exactitude	• Conception • Performance • Ergonomie • Qualité de service • Maintenance opérationnelle
Permettre l'accès aux entités autorisés	• Confidentialité • Intégrité	• Contrôle d'accès • Authentification • Contrôle d'erreur, de cohérence • Chiffrement • Détection, prévention d'intrusion, virus
Prouver des actions	• Non répudiation • Imputabilité • Tracabilité • Authenticité • Conformité aux lois	• Certification • Enregistrement, tracabilité • Signature électronique • Mécanisme de preuves

Question 3 :

Origine	cible	conséquence
Erreur	Individu	Atteinte à la dignité de l'individu Incitation à la haine raciale Vol d'identité
Accident	Organisation	Manipulation et destruction de l'information Atteinte au secret professionnel Diffusion de contenu illicite Fraude financière Perte d'intégrité
Malveillance	Etats	Chantage Cyberterrorisme Sabotage Escroquerie Atteinte à la disponibilité Détournement de fonds Rupture de confidentialité

Question 4 :

La protection de la vie privée (Privacy) est souvent définie comme la capacité de protéger des informations sensibles sur des informations personnellement identifiables, alors que la protection est en réalité un élément de sécurité. D'autres travaux le définissent comme le droit d'être laissé seul. Pourtant, cela ne couvre pas la vie privée d'aujourd'hui dans un monde centré sur les données, d'où la confusion. Dans l'industrie, la vie privée se concentre vraiment sur les concepts suivants:

- Quelles données devraient être collectées?
- Quelles sont les utilisations permises?
- Avec qui pourrait-il être partagé?
- Combien de temps les données doivent-elles être conservées?
- Quel est le modèle de contrôle d'accès granulaire approprié?

Question 5 :

a) Pour éviter le conflit d'intérêt, car une des tâches du responsable de la sécurité informatique et de s'assurer que la configuration des systèmes est la plus sécuritaire possible.

b)

- Les attaques venant de l'intérieur
- Les failles qui ne sont pas encore connues (vulnérabilités non découvertes, nouveaux virus, etc.
- Les erreurs de procédures des usagers
- Une politique de sécurité dont l'analyse de risques n'a pas identifié les risques les plus importants, et qui ne prévoit aucune contre-mesure procédurale ou technique pour les réduire.
- etc.

c) N'importe quelle de ces réponses est acceptable (en dépendant des hypothèses que vous faites) :

- Les dirigeants et décideurs de la compagnie (y compris l'exécutif) car ils n'ont pas identifié ni correctement évaluer la menace (le compétiteur) et les impacts (pertes de revenus).
- Le responsable (administratif) de la sécurité informatique qui, les risques et impacts étant bien identifiés par ses patrons, n'a pas établi clairement dans la politique de sécurité que ce genre d'information ne devrait pas circuler via l'Internet.
- L'utilisateur (l'assistant) qui, malgré que la politique de sécurité indiquait clairement le contraire, a quand même envoyé des informations confidentielles par l'Internet.
- Le responsable (technique) de la sécurité informatique qui, connaissant les risques technologiques associés à l'utilisation d'Internet et sachant qu'il y a un besoin réel et légitime d'envoyer des données confidentielles par Internet, n'a pas soit a) déconseillé aux décideurs de permettre cette pratique ou b) prévu des contre-mesures (VPN, chiffrement, etc.) pour en réduire les risques.