TD Sécurité Informatique

1. Définir la notion d'intégrité des données ainsi que les objectifs du contrôle d'intégrité.

L'intégrité est l'état d'une chose qui est demeurée intacte. Pour ce qui concerne des données, l'objectif du contrôle d'intégrité est de vérifier qu'elles n'ont pas été altérées tant de façon intentionnelle qu'accidentelle.

2. Quelles relations existent entre les critères d'intégrité et de confidentialité ?

La confidentialité des données est le maintien du secret des informations. L'information n'a pas été modifiée de manière non autorisée (intégrité), l'information n'est pas compréhensible par des personnes non autorisées (confidentialité). Les critères d'intégrité et de confidentialité sont complémentaires, lorsqu'ils sont réalisés par des fonctions *ad hoc* de sécurité, ils permettent de développer la confiance dans la véracité de l'information.

3. Dans quelle mesure la notion de qualité des données est-elle liée à celle de sécurité ?

La qualité est généralement une caractéristique d'excellence, reflétant une valeur, une compétence. Dans la mesure où des données possèdent un certain degré de sécurité et satisfont des exigences de disponibilité, d'intégrité ou de confidentialité, elles possèdent un degré intrinsèque de qualité et elles permettent d'offrir des services de qualité.

4. Parmi les critères de sécurité suivants, lequel n'est pas adapté à un système d'information ?

A) Confidentialité B) Intégrité √ C) Insolvabilité D) Non-répudiation

5. Sur quels principes se fonde la réalisation d'attaques informatiques ?

La réalisation d'attaques informatiques se fonde sur le leurre, le détournement, l'usage abu-sif des technologies, la manipulation d'information, l'exploitation des failles et vulnérabilités, l'usurpation d'identités et de paramètres de connexion d'ayants droit.

6. Pourquoi qualifie-t-on un virus de « polymorphe » ?

Un virus polymorphe est un virus qui change de signature (d'apparence) à chaque infection, ce qui rend sa détection difficile.

7. Quels sont les points communs entre un virus, un cheval de Troie, une bombe logique et un logiciel espion ?

Il s'agit de logiciels malveillants dont la charge et le mode de réalisation varient en fonction de la finalité.

Un cheval de Troie ne se duplique pas, tandis que la réplication caractérise un virus. Une bombe logique est un virus dont la charge malveillante se déclenche à une date ou selon un événement particulier.

8. Parmi les attaques informatiques suivantes quelle est celle qui peut être qualifiée d'attaque passive ?

A) Modification √ B) Interception C) Fabrication D) Interruption
E) Destruction

9. Parmi les infrastructures qui composent un système d'information laquelle ne peut être concernée par une cyberattaque ?

A) Matérielle B) Réseau C) Logicielle

D) Humaine E) Organisationnelle

Réponse : E

10. Comment les crypto-monnaies contribuent à la cybercriminalité ?

Réponse

Les crypto-monnaies contribuent à la cybercriminalité car elles permettent d'effectuer des transactions financières tout en préservant l'anonymat de leur propriétaire. Cela offre une obscurité propice à la criminalité économique qui constitue une couche de protection et d'isolation car les détenteurs de crypto-monnaies ne pourront être identifiés ou localisés. Ainsi ils ne peuvent être inquiétés par des forces de justice et police, ils échappent aussi aux systèmes de régulation et de contrôles des systèmes financiers.

Les crypto-monnaies bénéficient de cours de change qui se monnaient en dollars ou euros, de ce fait elles peuvent intervenir dans des circuits de blanchiment de l'argent sale issu de la criminalité. Cela contribue à la performance criminelle et au renforcement des acteurs criminels.

12. Parmi les assertions suivantes quelle est celle qui ne caractérise pas la sécurité informatique d'une organisation ?

A) Une vision à long terme B) Un mal nécessaire

C) Un compromis D) Du bon sens

Réponse : B

13. Parmi les propositions suivantes quelle est celle qui correspond le mieux au besoin de gérer la sécurité ?

A) Traiter la sécurité comme une exigence du business.

B) Appréhender et traiter la sécurité comme un processus continu.

C) Appréhender et traiter la sécurité comme un processus discontinu.

D) Appréhender et traiter la sécurité comme un processus connu.

Réponse : B

14. Quels sont les éléments constitutifs d'une politique de sécurité ?

Réponse

Les principaux éléments constitutifs sont : le champ d'application de la politique, les responsabilités, les procédures d'implémentation et de contrôle.

15. Laquelle des propositions suivantes ne concernent pas une politique de sécurité ?

A) Simple et compréhensible B) Aisément réalisable

C) Facilement maintenable D) Vérifiable et contrôlable

E) Approuvée par l'ensemble du personnel

Réponse : E

16. Quels sont les critères de sécurité qui correspondent le mieux à la notion de sûreté de fonctionnement ?

Réponse

Ce sont les critères de disponibilité et intégrité

17. Les mots de passe devraient être :

A. Assignés par l'administrateur de la sécurité.

B. Changés de façon régulière.

C. Réutilisés afin d'assurer que les utilisateurs ne les oublient pas.

D. Montrés sur l'écran pour que l'utilisateur puisse s'assurer que le saisi a été correct.

Réponse : B

18. Comment est-ce que la cybercriminalité peut affecter l'intégrité morale et physique d'un individu ?

Réponse

Par des actions portant atteintes aux personnes de manière directe ou indirecte ayant des impacts psychologiques (diffamation, harcèlement, manipulation, chantage, escroquerie économique, escroquerie sentimentale, diffusion de contenus choquants, atteintes pouvant conduire la personne au suicide…) ou par le biais de cyberactions sur des environnements physiques qui mettent en danger les personnes (accidents, explosion, déraillement d'un train, prise de contrôle à distance d'un moyen de transport, crash d'un avion…).

19. Quelles sont les caractéristiques principales d'un cybercrime ?

Réponse

Il s'agit d'un crime commis à distance, ou les technologies de l'information et de la communication peuvent être le moyen du crime et/ou la cible du crime.

C'est un crime qui s'effectue au travers du cyberespace. Le plus souvent le criminel est caché derrière un écran et agit *via* de multiples intermédiaires techniques.

Le cybercrime est facilité notamment par le fait :

• que tous les pays ne disposent pas forcément de la même volonté politique de lutter contre la cybercriminalité, ni des structures organisationnelles ou des ressources permettant de le faire ;

• que les procédures liées à l'entraide internationale des forces de justice et de police sont souvent complexes et longues ;

• que les traces numériques peuvent être brouillées, effacées ou fausses. De plus, les traces numériques sont difficiles à collecter, interpréter. Elles ne permettent pas toujours de remonter jusqu'à l'identité des criminels ;

• que les cybercrimes, se réalisent le plus souvent en impliquant de multiples acteurs aux compétences particulières et savoir-faire spécialisés dans des tâches spécifiques, séparées et restreintes (qui prises isolément peuvent paraître relativement mineures). Ces acteurs se regroupent en fonction de projets criminels à durée déterminée. Ils se constituent en équipes virtuelles réparties dans le monde entier et travaillent ensemble en fonction de missions ciblées, sur la base du recrutement des compétences ou de l'usage d'outils nécessaires pour mener à bien une activité criminelle, en prenant le moins de risques possibles.

20. Quels sont les facteurs et les acteurs qui contribuent à déterminer le niveau de protection des ressources informatiques d'une organisation ?

Réponse

Les principaux *facteurs* sont :

– L'importance, la valeur de la ressource à protéger par rapport au métier et besoin de l'organisation.

– Le niveau de dépendance de l'organisation à la ressource considérée (il peut s'agir de processus, de fonctions, de personnes…).

– Le fait qu'une ressource puisse être soumise à une réglementation particulière (contraintes légales).

– Les contraintes financières.

– L'existence de personnes compétentes au sein de l'organisation pour prendre en charge cette tâche.

Les principaux *acteurs* sont les dirigeants de l'entreprise au niveau stratégique (top manager, comité de direction, conseil d'administration), la responsable sécurité au niveau opérationnel ainsi que les responsables métier et les propriétaires des ressources.

21. Expliquer comment le concept de « séparation des tâches » contribue à la sécurité informatique d'une organisation.

Réponse

En matière de sécurité informatique, la séparation des tâches contribue à prévenir des fraudes d'origine interne dues à des pouvoirs excessifs accordés à une même personne qui s'avère être malhonnête (notion de moindre privilège).