Nom : _____
Note : _____ / _____

Examen M2 WedSci

Partie 1

1

Les principaux principes de base qui guident à la fois la mise en oeuvre et l'évaluation de la sécurité des systèmes d'information sont :

- A.
  L'authentification, l'intégrité et la confidentialité
- B.
  La disponibilité, la confidentialité et la non-répudiation
- C.
  L'intégrité, la confidentialité et la disponibilité
- D.
  La disponibilité, l'authentification et l'intégrité

Valeur en points de la réponse: 2.0 points
Corrigé: C

2

Lors de la mise en oeuvre d'une PSSI, le débat autour de l'échelle convenable pour caractériser des critères de sécurité s'éternise. Sélectionnez les 2 seules propositions cohérentes parmi les quatre.

- A. Critère : Disponibilité Echelle : Privé, réservé, public Critère : Intégrité Echelle : 24h, 72h, plus de 72h
- B. Critère : Confidentialité Echelle : Individuel, Interne, Partenaire, Public Critère : Disponibilité Echelle : Opérationnel, dégradé, inaccessible
- C. Critère : Intégrité Echelle : Conforme, incomplet, falsifié Critère : Disponibilité Echelle : en ligne, hors ligne, suspendu, résilié
- D. Critère : confidentialité Echelle : conforme, incomplet, falsifié Critère : authentification Echelle : biométrie, token, login/mot de passe

Valeur en points de la réponse: 2.0 points
Corrigé: B,C

3

Parmi les assertions suivantes, cochez celles qui s'appliquent à l'externalisation des applicatifs de l'infrastructure locale d'Entreprise vers le Cloud (3 réponses correctes maximum).

- [ ] A. L'externalisation des applicatifs vers le Cloud permet de réduire des coûts périodiques et arbitrés (achats de matériels, maintenance) nécessaires au maintien d'une infrastructure interne dans l'Entreprise, mais elle entraîne l'augmentation de coûts forfaitaires permanents (accès Internet, abonnement aux services Cloud).

- [ ] B. Lorsqu'une Entreprise externalise ses applicatifs vers le Cloud, il suffit donc que chaque poste de travail dispose d'une connexion Internet avec une adresse IPv6 pour s'y connecter de n'importe quel endroit. En revanche, l'Entreprise perd ainsi toute possibilité d'administrer ses postes de travail, de créer des sous-réseaux, d'appliquer des règles d'accès spécifiques à chaque poste ou groupes de postes, etc.

- [ ] C. En augmentant le trafic réseau vers le Cloud, l'externalisation et l'Internet des objets induisent des latences qui sont à l'origine des dernières avancées en réseaux : généralisation de l'accès fibre optique, insertion de mini-Cloud au plus près des usagers (Edge Computing), mise en cache massive sur les équipements de transfert réseaux (Fog Computing), globalisation de la gestion des accès sans-fil (5G).

- [ ] D. L'externalisation réduit fortement tous les risques de sécurité accidentels (sauvegarde systématique en plusieurs endroits dans le Cloud, disponibilité accrue du fait de la redondance des accès, etc), mais elle augmente les risques de sécurité intentionnels (exposition directe de tous les postes de travail à Internet, dépendance à l'opérateur Cloud pour la garantie de la confidentialité, etc).

Valeur en points de la réponse: 2.0 points
Corrigé: A,C,D

4

La mise en oeuvre de la sécurité sur le critère de la disponibilité repose en grande partie sur la protection de l'accès aux ressources via le réseaux aux seuls terminaux, utilisateurs et trafics légitimes. Il s'agit donc en général de spécifier très clairement tous les accès autorisés et d'interdire par défaut tous les autres. Dans un contexte d'infrastructure locale, le pare-feu est placé à l'entrée du réseau de l'Entreprise. Dans un contexte d'externalisation, les postes de travail sont éparpillés entre l'Entreprise, les employés mobiles et les télé-travailleurs. Dans ces conditions, où doit être implémenté le pare-feu matérialisant la politique propre de l'Entreprise ?

- A. Dans les serveurs alloués à l'Entreprise par l'hébergeur Cloud et à l'entrée du réseau de l'Entreprise
- B. Sur chaque poste de travail mobile et à l'entrée du réseau local de l'Entreprise.
- C. Sur chaque poste de travail appartenant à l'Entreprise ainsi que sur les serveurs alloués à l'Entreprise par l'hébergeur Cloud.
- D. Il n'y a plus besoin de pare-feu, car l'opérateur Cloud s'occupe de toute la protection nécessaire.

Valeur en points de la réponse: 2.0 points
Corrigé: C

5

Dans un réseau local basé sur une architecture classique reliant le routeur à deux commutateurs principaux (un par bâtiment), tous les commutateurs secondaires sont directement reliés au commutateur principal du bâtiment dans lequel ils se trouvent et chaque poste de travail est obligatoirement connecté à un de ces commutateurs secondaires. Quelles affirmations (deux) sont vraies parmi les quatre.

- [ ] A. Si on suppose que le taux de perte est uniforme pour toutes les liaisons, alors le taux de perte estimé pour tout trafic allant d'un poste de travail vers Internet est à peu près le quadruple du taux de perte d'une liaison élémentaire.
- [ ] B. Si la connexion Internet a un débit inférieur à celui des liaisons dans le réseau local, alors le délai estimé entre deux postes de travail quelconque à l'intérieur du réseau est forcément plus petit que le délai vers Internet à partir de l'un quelconque de ces postes.
- [ ] C. Si la connexion Internet a un débit inférieur à celui des liaisons dans le réseau local, alors le débit vers Internet à partir de l'un quelconque des postes de travail ne dépend que du débit de la carte de ce poste de travail.
- [ ] D. Si l'on ajoute une liaison directe entre les deux commutateurs principaux des bâtiments, alors le taux de perte global pour tout trafic allant d'un poste de travail vers Internet augmente.

Valeur en points de la réponse: 2.0 points
Corrigé: A,B

6

En cryptographie asymétrique, laquelle des assertions suivantes est fausse :

- ( ) A. Les deux clés sont interchangeables tant qu'aucune d'elles n'a été rendue publique.
- ( ) B. Lorsqu'on chiffre avec la clé privée, ce n'est pas dans le but d'assurer la confidentialité.
- ( ) C. Elle est plus adaptée que la cryptographie symétrique pour le chiffrement de flux d'applications temps réel.
- ( ) D. Si l'on démontre que P = NP alors la fin de l'utilisation de la cryptographie asymétrique comme outil de sécurité valide pour le commerce électronique ne sera plus qu'une question de temps.

Valeur en points de la réponse: 2.0 points
Corrigé: C

7

Cochez toutes les affirmations vraies sur le certificat électronique.

- [ ] A. Le certificat électronique contient la clé publique du serveur auquel il a été attribué afin que tous les clients puissent l'utiliser pour lui envoyer des données chiffrées.
- [ ] B. Le certificat électronique contient également la clé privée du détenteur.
- [ ] C. La validité du certificat électronique est assurée par la présence d'un Hash des informations sur le détenteur chiffré avec la clé privée de l'autorité de certification (sceau signé). Il suffit d'utiliser le certificat de l'autorité de certification pour vérifier la signature, et le Hash déchiffré peut être comparé à un Hash des informations du certificat du détenteur pour en vérifier l'intégrité et donc l'authenticité.
- [ ] D. Tant que l'Entreprise ne change ni de nom, ni d'adresse, il n'est pas nécessaire de remplacer les certificats attribués à ses serveurs, même plusieurs années après leur édition.

Valeur en points de la réponse: 2.0 points
Corrigé: A,C

8

Un seul des mécanismes suivants n'est pas réellement un paradigme faisant partie de nouvelles architectures de réseaux. Cochez-le.

A. La radio-logicielle (Software Defined Radio) est une approche qui consiste à remplacer les dispositifs de codage et décodage d'ondes radios spécifiques à différentes fréquences, par un logiciel opérant sur l'ensemble des bandes de fréquences. Ainsi, il suffit d'embarquer ce logiciel sur une carte programmable pour qu'il puisse émuler à volonté un point d'accès Wifi, un terminal bluetooth, une station de base 4G, etc.

B. Le Named Server Networking (NSN) est un paradigme qui permet de traiter directement avec des serveurs via leur nom plutôt que via leur adresse IP. Lorsqu'un utilisateur effectue une recherche google par exemple, au lieu que sa requête soit envoyée à l'adresse IP du serveur de google, la requête est transmise au NSN dans le Cloud qui détermine à quelle machine envoyer la requête afin qu'elle soit traitée.

C. Le Software Defined Networking (SDN) est un paradigme qui permet réalisation l'organisation logique d'un réseau via un logiciel directement à partir d'un serveur dédié (notamment dans le Cloud). Ainsi, les terminaux connectés au Cloud peuvent être affectés à des sous-réseaux, auxquels peuvent être appliqués des règles d'accès, des capacités particulières en fonction de la politique du détenteur.

D. La virtualisation des fonctions réseaux (Network Function Virtualisation) est une technique qui consiste à remplacer les équipements opérant au coeur du réseau par un ensemble de logiciels déployés directement dans le Cloud. Ainsi, le trafic en provenance des terminaux est récupéré via des super-canaux filaires (fibre) ou sans-fil (4G/5G) puis traités dans le Cloud avant leur retransmission dans les points d'intérêt du réseau.

Valeur en points de la réponse: 2.0 points
Corrigé: B

9

Parmi les assertions suivantes portant sur la sécurité des systèmes d'information et du réseau, plusieurs sont correctes et plusieurs sont fausses. Cochez au moins une réponse correcte pour obtenir les 2 points.

- A. Le pare-feu réseau est un dispositif de protection efficace contre tout trafic provenant d'un segment du réseau vers les autres segments du réseau. En particulier, il peut bloquer les tentatives d'intrusions en provenance d'Internet vers le réseau local, y compris lorsque les employés utilisent une passerelle 4G sur le poste de travail relié au réseau de l'Entreprise.

- B. Le pare-feu applicatif est un dispositif intrusif qui accède aux messages transmis dans un réseau IP et en analyse le contenu, y compris dans les sections autres que les en-têtes, afin de détecter des séquences interdites ou malicieuses. A ce titre, sa présence dans un réseau doit être explicitement notifié aux utilisateurs au même titre que la vidéo-surveillance.

- C. La cryptographie asymétrique garantit une sécurité des échanges via les réseaux sûre à 100% pour tous les critères de sécurité, à l'exception de la disponibilité. Les principales failles viennent du système d'exploitation, des langages de programmation, des programmeurs et administrateurs laxistes.

- D. Avec l'avènement du Cloud qui généralise l'externalisation des applicatifs et qui permet la connexion des utilisateurs de n'importe où, souvent même avec leur propre machine (BYOD - Bring Your Own Device) en télétravail sur laquelle ils sont administrateurs et peuvent installer n'importe quel application, la mise en place de pare-feux applicatifs ne sert plus à rien.

Valeur en points de la réponse: 2.0 points
Corrigé: B,C

10

Lors de la mise en place d'une politique de sécurité du système d'information, quelle est le bon ordre à suivre dans la réalisation des étapes ?

- A. Analyse et qualification des risques Analyse des événements redoutés Analyse des scénarios de menaces Détermination des critères et des échelles relatifs Evaluation des mesures en place et réduction des risques Préconisation des mesures supplémentaires
- B. Analyse des événements redoutés Analyse des scénarios de menaces Analyse des scénarios de menaces Analyse et qualification des risques Evaluation des mesures en place et réduction des risques Formation des utilisateurs Préconisation des mesures supplémentaires
- C. Détermination des critères et des échelles relatifs Analyse des scénarios de menaces Analyse des événements redoutés Analyse et qualification des risques Evaluation des mesures en place et réduction des risques Formation des utilisateurs
- D. Détermination des critères et des échelles relatifs Analyse des événements redoutés Analyse des scénarios de menaces Analyse et qualification des risques Evaluation des mesures en place et réduction des risques Préconisation des mesures supplémentaires Formation des utilisateurs

Valeur en points de la réponse: 2.0 points
Corrigé: D