Quiz RRSI

Durée : 1h30mn

Parie 1 : Protection des données *(encerclé la ou les bonnes reponses)*

1) Que fait un ransomware sur votre PC ? *
   a) Il verrouille le disque dur avec un mot de passe
   b) Il crypte les données
   c) Il est envoyé automatiquement à toutes les adresses e-mail
2) Le Social Engineering est…*
   a) L'influence interpersonnelle afin d'obtenir des informations sensibles en matière de sécurité
   b) L'influence interpersonnelle afin d'obtenir des informations sensibles en matière de sécurité un logiciel malveillant nommé d'après ses inventeurs qui sont d'anciens ingénieurs
   c) Un logiciel malveillant qui se propage par l'intermédiaire des réseaux sociaux
3) Un Drive-by download est dangereux car…*
   a) Il peut se cacher dans les bannières sur les sites Web
   b) Ce logiciel malveillant fonctionne avec n'importe quel programme e-mail
   c) Il se propage via WLAN
4) Un logiciel antivirus protège le réseau d'entreprise le plus efficacement lorsque...*
   a) Il est installé et tenu à jour sur tous les PC et serveurs.
   b) Il contrôle toutes les données entrantes exclusivement sur le serveur en même temps que le firewall.
   c) Deux programmes antivirus différents sont utilisés simultanément sur les PC.
5) Quand faut-il faire une mise à jour des logiciels ? *
   a) Dès que l'éditeur fournit une mise à jour

b) Quand l'éditeur me le demande par e-mail

c) Seulement quand il y a une nouvelle version du système d'exploitation

6) Quelles passerelles d'entrée potentielles sont souvent oubliées lors de la protection du réseau de l'entreprise ? *

a) Les imprimantes réseau, parce qu'elles sont accessibles via le réseau

b) Les souris sans fil sont souvent exploitées par les mouseware

c) Les cartes graphiques qui sont souvent les cibles d'attaques de virus en raison de mises à jour manquantes

7) Que faire des alertes ? *

a) Tous les messages d'alerte doivent être pris en compte et traités. Les messages incompréhensibles doivent être discutés avec le responsable informatique de l'entreprise ou avec le partenaire IT.

b) Les utilisateurs et les administrateurs ne doivent pas s'occuper du traitement des messages d'alerte. Ceux-ci sont traitées par les responsables IT ou les collaborateurs du partenaire IT.

c) Les systèmes d'exploitation et les logiciels antivirus génèrent trop de messages d'alerte inutiles et réduisent l'efficacité. Il convient avant tout de s'occuper des messages hautement prioritaires.

8) Quel est le rôle d'un firewall ? *

a) Il supprime les virus et les chevaux de Troie des e-mails

b) Il surveille le trafic réseau

c) Il empêche les composants du PC de surchauffer

9) La sécurité du WLAN de l'entreprise est augmentée lorsque...*

a) La direction dispose de droits de réseau étendus.

b) Les visiteurs ont besoin d'un autre mot de passe WLAN que les collaborateurs.

c) Les visiteurs et les collaborateurs utilisent des réseaux séparés.

10) Comment créer des backups sécurisés ? *

a) Les backups automatiques dans le cloud sont généralement plus sûrs et plus pratiques que les sauvegardes de données locales.

b) Les backups doivent être effectués via le réseau. Le stockage de backup doit être intégré à tout moment au réseau afin que le backup puisse par exemple avoir lieu la nuit.

c) Les PC contiennent souvent des données d'entreprise importantes. C'est pourquoi une sauvegarde complète du disque dur de chaque PC devrait être effectuée chaque jour.

11) Les connexions et les accès à distance sont sécurisés lorsque...*

a) Tous les utilisateurs et administrateurs utilisent une authentification à deux facteurs pour se connecter.

b) Les collaborateurs n'ont accès au réseau d'entreprise qu'à partir de réseaux WLAN sécurisés et non du WLAN public, p. ex. à l'hôtel.

c) Le mot de passe est conforme aux spécifications pour des mots de passe sûrs et est régulièrement modifié.

12) La sécurité du réseau peut être renforcée si...*

a) Dans la mesure du possible, les collaborateurs connectent leurs appareils au réseau via un LAN au lieu d'un WLAN.

b) Le réseau d'entreprise est segmenté en différents secteurs.

c) L'entreprise ne propose pas de WLAN pour les visiteurs.

13) En entreprise, quels sont les principaux facteurs de risque en sécurité informatique ?

a) Défaillance du matériel

b) Erreurs humaines et mauvais comportement

c) Les événements naturels

d) Panne d'électricité

14) La tentative d'infraction informatique est-elle condamnée au Benin ?

a) Oui, par les mêmes peines que l'infraction

b) Oui, par des peines moindres

c) Non, la loi ne précise pas

15) Est-ce que cette affirmation est correcte : « Les virus existent seulement sous Windows, les autres systèmes d'exploitation et les PDA ne sont pas touchés ?»

a) Vrai
b) Faux

16) Quel est le type d'accès FTP dans lequel l'utilisateur n'a pas les autorisations pour répertorier le contenu des dossiers mais il peut accéder au contenu s'il sait le chemin et le nom des répertoires ?

a) Anonymous FTP
b) Secure FTP
c) Blind FTP

17) Un utilisateur se plaint d'une connexion Internet lente. Il vérifie l'interface externe du routeur en remarquant plusieurs connexions semi-ouvertes. Quel type d'attaque cela décrit-il ?

a) Attaque DDOS.
b) Sniffing
c) SYN flooding.

18) Lequel des énoncés suivants décrit une attaque par injection de LDAP ?

a) Manipuler les requêtes LDAP pour obtenir ou modifier les droits d'accès.
b) Utiliser XSS pour diriger l'utilisateur vers un serveur LDAP falsifié.
c) Envoi de débordement de tampon pour le service de requête LDAP.
d) Création d'une copie des informations d'identification de l'utilisateur au cours de la session d'authentification LDAP.

19) Quelle procédé permettant d'assurer la non-répudiation des données ?

a) La signature électronique
b) Le hachage des mots de passes
c) Le certificat électronique

20) Lequel décrit une vulnérabilité logicielle exploitant une faille de sécurité avant qu'un patch de protection ne soit disponible ?

a) Zero day attack
b) Buffer overflow
c) Mystification d'adresse MAC

Parie 2 : Sécurité informatique *(encerclé la ou les bonnes reponses)*

1) Qu'est-ce que le RGPD ? Quel est organique qui s'occupe de la protection des données à caractère personnel au BENIN ?

Rep :

2) Qu'est-ce que ISO 27001 ? Quel est son avantage pour les entreprises ?

Rep :

3) Qu'est-ce que le Système de Gestion de la Sécurité Informatique et son avantage en entreprise ?

Rep :

4) Citez deux (2) logiciels de scan de vulnérabilité reseau et deux (2) de monitoring reseau que vous maitrisez correctement :

Rep :

5) Le premier objectif indispensable du test d'un plan de continuité des activités (PCA) est :

a) Identifier les limites du plan de continuité d'affaires.
b) Se préparer à tous les scénarios de désastre possibles.
c) Garantir que tous les risques restants sont traités.
d) Familiariser des employés avec le plan de continuité d'affaires.

6) Dans le cadre d'installation d'un système de détection d'intrusion (IDS), qu'est ce qui est le plus important ?

a) Prévenir contre les attaques de déni de service (Dos).
b) Identifier les messages qui doivent être mis en quarantaine.
c) Minimiser les erreurs dans les rejets.
d) Localiser correctement l'IDS dans l'architecture de réseau.

7) Lequel des services suivants doit être désactivé pour empêcher les hackers d'utiliser un serveur Web comme un relais de messagerie ?

a) SMTP
b) POP3
c) SNMP
d) IMAP

8) Quel type d'attaque nécessite un attaquant pour renifler un réseau (sniffing) ?

a) Man-in-the-Middle
b) MAC flooding
c) DDoS
d) Zero day exploit

9) Lequel des éléments suivants permet de faire un backdoor caché pour accéder aux postes de travail sur Internet ?

Cheval de Troie
Bombe logique
Firmware
Ver

10) Lequel des éléments suivants est utilisé pour effectuer un déni de service (DoS) ?

Rootkit

Bombe logique

Botnet

Port redirection

11) Quels sont les algorithmes cryptographiques utilisables par le protocole SSH ?

DES et AES

RSA et AES

RSA et DES

12) Quelle technique permettant d'assurer l'intégrité des données ?

La signature électronique

Le certificat électronique

Le chiffrement

13) La signature DSS utilise quel algorithme de hachage ?

MD5

SHA-2

SHA-1

N'utilise pas d'algorithme de hachage

14) _____ est une forme de virus explicitement conçue pour se cacher de la détection par un logiciel antivirus.

Virus furtif

Virus polymorphe

Virus parasite

Virus de macro

15) Indiquez si l'énoncé suivant est vrai : Un virus macro est indépendant de la plate-forme.

Vrai

Faux

16) Indiquez si l'énoncé suivant est vrai : Les virus macro infectent les documents et non des parties de code exécutables.

Vrai

Faux

17) Un _____ est un programme qui prend le contrôle d'un autre ordinateur connecté sur Internet, puis utilise cet ordinateur pour lancer des attaques.

Ver

Zombie

Virus

Porte dérobée (Trap doors)

18) Quelle est la taille de votre signature RSA après les traitements MD5 et SHA-1 ?

42 octets

32 Octets

36 Octets

48 Octets

19) Dans la sécurité informatique, _____ signifie que les systèmes actifs informatique ne peuvent être modifiés que par des parités autorisées.

La confidentialité

L'intégrité

La disponibilité

L'authenticité

20) Lequel des programmes suivants est un programme malveillant indépendant qui ne nécessite aucun programme hôte ?

Porte à piège

Cheval de Troie

Virus

Ver

Fin.