**QUESTIONNAIRE CYBERSECURITE**

**1. Sélectionner les enjeux de la Cybersécurité ?**

Réponses possibles :

a. Augmenter les risques pesant sur le système d’information ;

b. Révéler les secrets ;

**c. Rendre difficile la vie des utilisateurs en ajoutant plusieurs contraintes comme les mots de passe longs et complexes ;**

**d. Protéger le système d’information.**

**2. Si vous étiez victime d’une attaque cybercriminelle, quelles pourraient être les conséquences**

(impacts) sur votre vie privée (deux exemples) ?

Usurpation d’identité

Utilisation des données personnelles

**3. Citer les trois principaux besoins de sécurité.**

Mots de passes forts

Antivirus

Parefeu physique

(après avoir relu : disponibilité intégité confidentialité ?)

**4. Choisir la (ou les) phrase(s) correcte(s)**

Réponses possibles :

a. Le chiffrement permet de garantir que la donnée sera toujours disponible/accessible ;

**b.** **La sécurité physique permet d’assurer la disponibilité des équipements et des données** ;

c. La signature électronique permet de garantir la confidentialité de la donnée ;

**d.** **Les dénis de service distribués (DDoS) portent atteinte à la disponibilité des données.**

**5. Entourer les éléments facilitateurs des fraudes internes :**

Réponses possibles :

**a. Des comptes utilisateurs partagés entre plusieurs personnes** ;

b. L’existence de procédures de contrôle interne ;

**c. Peu ou pas de surveillance interne ;**

d. Une gestion stricte et une revue des habilitations.

**6. Entourer les éléments qui peuvent réduire ou empêcher des fraudes internes :**

Réponses possibles :

**a. Une gestion stricte et une revue des habilitations ;**

**b. Une séparation des rôles des utilisateurs ;**

c. Peu ou pas de surveillance interne ;

**d. Des comptes utilisateurs individuels pour chacun.**

**7. Citer deux moyens (vecteurs d’infection) par lesquels les virus informatiques peuvent être transmis d’un système compromis (ou d’un attaquant) à un système sain.**

Support externe personnel tel qu’une clé usb

Mail frauduleux (pourriel)

**8. Dans un réseau, l’usage du BYOD peut entrainer (choisir la (ou les) proposition(s) vraie(s)) :**

Réponses possibles :

**a. Une restriction du périmètre à sécuriser ;**

**b. La propagation de codes malveillants ;**

**c. La fuite de données de l’entreprise** ;

d. Une meilleure sécurité du SI.

**9. Un « pare-feu » peut être aussi bien matériel (appliance dédiée) que logiciel ?**

Réponses possibles :

**a. Vrai ;**

b. Faux.

**10. Entourer la (ou les) bonne(s) mesure(s) de sécurisation de l’administration :**

Réponses possibles :

a. Rendre les interfaces d’administration disponibles à tous depuis Internet ;

b. Tous les administrateurs doivent utiliser le même compte pour se connecter ;

**c. Utiliser un réseau dédié pour l’administration ;**

**d. Authentifier mutuellement les postes des administrateurs et les serveurs à administrer.**

**11. Quelle est la technologie la plus appropriée pour sécuriser son accès Wifi :**

Réponses possibles :

a. WEP;

b. WPA ;

c. WPS;

**d. WPA2**.

**12. Laquelle (ou lesquelles) des expressions suivantes est (sont) vraie(s) pour un logiciel téléchargeable**

?

Réponses possibles :

a. Toujours gratuit ;

**b. Peut-être « open source » ;**

**c. Peut contenir des logiciels espions ;**

**d. Peut-être un programme malveillant.**

**13. Citer une bonne pratique de configuration de son antivirus :**

Réponses possibles :

a. Avoir un antivirus d’un éditeur connu ;

b. Avoir un jour installé un antivirus ;

**c. Tenir son antivirus à jour (mise à jour des signatures et du moteur)** ;

d. Interdire l’analyse antivirale à certains répertoires ou périphériques.

**14. Sélectionner la (ou les) proposition(s) vraie(s) parmi les suivantes. Un antivirus :**

Réponses possibles :

a. Peut détecter tous les virus et programmes malveillants, y compris ceux non découverts ;

b. Protège de toutes les menaces ;

**c. Ne peut détecter que les virus qui sont connus dans sa base de signatures ;**

**d. Doit être actif, et à jour pour être utile**.

**15. Sélectionner le (ou les) moyen(s) de durcissement d’une configuration :**

Réponses possibles :

**a. Modifier les mots de passe par défaut ;**

b. Désinstaller les logiciels inutiles ;

c. Activer le mode « débogage USB » sur les téléphones ;

**d. Sécuriser le BIOS à l’aide d’un mot de passe.**

**16. Entourer la (ou les) bonne(s) pratique(s) pour les mots de passe :**

Réponses possibles :

a. J’enregistre mes mots de passe sur chaque navigateur Internet ;

**b. Je crée un mot de passe long et complexe dont je peux me souvenir facilement ;**

c. J’écris mon mot de passe sur un post-it que je cache sous mon clavier/PC ;

**d. J’utilise un porte-clés de mots de passe.**

**17. Entourer la (ou les) bonne(s) pratique(s) de navigation sur Internet :**

Réponses possibles :

a. Je suis victime de ransomware, je paye la rançon ;

**b. J’évite de communiquer avec des inconnus ;**

c. J’accepte toutes les demandes sur les médias sociaux ;

d. Je donne mon mot de passe de messagerie à « l’administrateur » lorsqu’il me le demande.

**18. Citer deux moyens de sécurisation physique des biens/équipements :**

Réponses possibles :

a. Mettre les équipements sensibles dans une salle sans contrôle d’accès ;

**b. Attacher les équipements sensibles avec des câbles de sécurité ;**

c. Nommer tous les équipements de la même façon ;

**d. Utiliser des filtres de confidentialité pour les écrans**.

**19. Choisir la (ou les) bonne(s) réaction(s) face à un incident de sécurité :**

Réponses possibles :

a. Désactiver/désinstaller son antivirus ;

**b. Appliquer les règles/consignes reçues par exemple dans la charte informatique ;**

**c. Chercher à identifier la cause de l’incident ;**

d. Désactiver son pare-feu (personnel par exemple).

**20. La sécurité est au cœur de l’implémentation de la famille de protocoles IP :**

Réponses possibles :

**a. Vrai ;**

b. Faux.

**21. Le chiffrement des données transportées est automatiquement pris en compte dans la famille**

**de protocole IP au niveau de la couche Transport :**

Réponses possibles :

a. Vrai ;

**b. Faux.**

**22. Lorsqu’un attaquant C peut écouter et modifier les informations échangées entre A et B, on parle d’ « écoute » :**

Réponses possibles :

**a. Passive ;**

b. Active ;

c. Hacktiviste ;

d. Discrète.

**23. Entourer un équipement qui permet de définir et contrôler les flux autorisés et interdits entre deux réseaux ?**

Réponses possibles :

a. Un routeur ;

**b. Un pare-feu ;**

c. Un hub ;

d. Un répartiteur de charge.

**24. Quel rôle un proxy (serveur mandataire) peut-il jouer en matière de sécurité ?**

Réponses possibles :

**a. Il peut mettre en cache des pages Internet déjà demandées ;**

**b. Il peut autoriser ou interdire certains flux applicatifs ;**

c. Il peut rechercher des éléments malveillants ;

d. Il peut chiffrer les communications.

**25. Quel équipement peut aider à se protéger des dénis de services distribués (DDoS) ?**

Réponses possibles :

a. Un antivirus ;

b. Un routeur ;

c. Un proxy ;

**d. Un répartiteur de charge.**

**26. Quelle technologie permet de créer une communication sécurisée entre deux réseaux en s’appuyant sur un réseau qui n’est pas de confiance ?**

Réponses possibles :

a. Internet ;

b. Wifi ;

**c. VPN ;**

d. 4G.

**27. Les VLAN sont des réseaux virtuels implémentés sur les routeurs :**

Réponses possibles :

a. Vrai ;

**b. Faux.**

**28. Un proxy me permet de masquer mon adresse interne vis-à-vis d’Internet :**

Réponses possibles :

a. Vrai ;

**b. Faux.**

**29. Comment s’appelle le processus de transformation d’un texte en clair en un texte illisible à l’aide d’un algorithme ?**

La cryptographie (chiffrement)

**30. Lorsque la clé utilisée pour transformer un texte en clair en texte illisible est la même pour rendre, le texte illisible en texte en clair, on parle de ?**

Réponses possibles :

a. Cloisonnement ;

b. Chiffrement asymétrique ;

**c. Chiffrement symétrique ;**

d. Virtualisation.

**31. Lorsque pour envoyer un message privé à Bob, Alice utilise la clé publique de Bob pour rendre « illisible » le « texte en clair », et que Bob utilise sa clé privée pour transformer le texte « illisible » en « texte en clair », on parle de ?**

Réponses possibles :

a. Chiffrement symétrique ;

b. Tokenisation ;

c. Envoi privé ;

**d. Chiffrement asymétrique**.

**32. Lors de la navigation sur Internet, les \_cookies\_ sont des fichiers temporaires créés et gérés par les navigateurs Web afin de stocker les informations concernant les utilisateurs telles que :**

Réponses possibles :

**a. Son identifiant ;**

**b. Les thèmes et les préférences d’affichage.**

**33. Les compétences recherchées en Cybersécurité sont uniquement techniques :**

Réponses possibles :

a. Vrai ;

**b. Faux**.

**34. Entourer les éléments qu’on peut retrouver dans un certificat électronique d’une entité :**

Réponses possibles :

a. Les noms, prénoms, URL de l’entité (ou son url) ;

b. La clé privée de l’entité ;

**c. La signature d’un tiers de confiance (des autorités de certification)** ;

**d. La période de validité du certificat.**

**35. Depuis Internet, lorsqu’un attaquant réussit à contourner les mécanismes d’authentification et à interroger directement la base de données par écriture de commandes spécifiques, on parle de :**

Réponses possibles :

a. Hacking ;

b. XSS (Cross Site Scripting) ;

**c. Injection SQL ;**

d. Malware.

**36. Lors de la navigation en https sur un site Web, il faut faire attention à :**

Réponses possibles :

a. La validité du certificat annoncé par le site (le certificat n’a pas encore expiré) ;

**b. L’autorité ayant accordé le certificat (par exemple, il ne faudrait que le certificat soit auto-signé ou issue d’une autorité non reconnue) ;**

**c. L’alerte de mon navigateur indiquant que le certificat présenté par le site n’est pas de confiance ;**

d. Il n’y pas de raison de faire attention ! « https » signifie que je peux naviguer en toute confiance.

**37. Quel équipement réseau peut être utilisé pour détecter une intrusion ?**

Réponses possibles :

**a. Un pare-feu ;**

b. Un IDS ;

**c. Un IPS ;**

d. Un antivirus.

**38. Choisir la (les) proposition(s) correcte(s) :**

Réponses possibles :

a. Il est plus facile d’attaquer un système que de le rendre invulnérable ;

b. Il est facile de créer un système sans aucune vulnérabilité ;

**c. Pour défendre un système, il suffit de le protéger de manière périmétrique ;**

**d. La « défense en profondeur » peut être appliquée pour protéger un système.**

**39. La Cybersécurité est un secteur ayant peu de perspective d’embauche :**

Réponses possibles :

a. Vrai ;

**b. Faux.**

**40. Cybermalveillance.gouv.fr est un dispositif permettant d’informer, prévenir et d’assiter :**

a. les Entreprises

b. les particuliers

**c. les deux**