CORRIGÉ

Chapitre 14

QCM

1. B. Le risque en sécurité informatique est défini par le produit de la vulnérabilité d'un système, de la menace qui pèse sur celui-ci et de l'impact qui peut en découler.

2. C. La méthode incrémentale sera privilégiée car c'est le type de sauvegarde requérant le moins d'espace de stockage.

3. C. En sécurité informatique, l'ingénierie sociale est une technique de manipulation psychologique utilisée pour obtenir une information confidentielle d'une personne (par exemple, se faire passer pour un salarié ou un prestataire ayant oublié son code d'accès).

4. A. On a coutume de dire que l'humain est le maillon faible de la chaîne de la sécurité. Des formations à la sécurité peuvent aider à réduire le risque lié au facteur humain, mais ne le rendent pas nul.

5. C. Les deux grandes catégories de risque en sécurité informatique sont les risques opérationnels et fonctionnels (liés aux métiers).

6. A. D. Les trois piliers de la sécurité informatique sont la confidentialité, l'intégrité (et non l'intégralité) et la disponibilité.

7. A. B. Le terme « actifs informationnels » regroupe les données stratégiques et sensibles de l'entreprise.

8. A. C. D. La bonne réaction face aux pourriels et aux arnaques est de se désabonner des listes de diffusion qui envoient ces messages, d'avoir ses logiciels de protection à jour (anti-spam, antivirus, etc.), et d'éviter de donner son adresse e-mail à des sites auxquels vous ne faites pas confiance. En aucun cas il ne faut répondre au courrier malveillant.

9. A. B. C. Les logiciels malveillants sont les virus, les vers, les chevaux de Troie, les rançongiciels et les espiogiciels.

10. A.B. La protection logicielle et matérielle du réseau local d'une entreprise est assurée par les logiciels antivirus, pare-feu, antispyware et détection d'intrusion, ainsi que par les serveurs mandataires, proxy pare-feu.

11. B. C. D. L'authentification au sein d'un réseau local d'une entreprise peut être faite par un mot de passe personnel (et donc en aucun cas par un mot de passe connu de plusieurs personnes – une équipe par exemple), et/ou par une carte à puce (ou un jeton) et/ou par de la biométrie (empreinte digitale, voix, rétine, etc.).

12. A. B. C. Les mesures de sécurité informatique sont un tout qui regroupe l'ensemble des solutions techniques misent en place (les logiciels et le matériel), ainsi que les règles édictées aux utilisateurs ainsi que les procédures à appliquer en cas de problème de sécurité.

13. B. C. Lorsque des données sont hébergées dans un cloud, l'entreprise propriétaire des données doit en assurer la protection (et non le fournisseur du cloud). Quel que soit le pays dans lequel les données sont localisées, leur niveau de protection doit satisfaire aux exigences de la politique de sécurité de l'entreprise. Les garanties de sécurité demandées par l'entreprise au

fournisseur du cloud (par exemple, règles de confidentialité, séparation des données des autres entreprises, chiffrement, rétablissement après sinistre, audits externes et certifications de sécurité…) peuvent faire l'objet d'un SLA.

14. A. B. C. Les mesures organisationnelles de sécurité informatique regroupent la liste de « qui peut faire quoi » appelée politique de sécurité, la liste des risques avec leur niveau de gravité (analyse d'impact), et enfin la liste des actions à mener en cas de problème de sécurité, selon le problème (plans de secours)

15. A. C. D. La sécurité d'un poste de travail passe par le fait d'avoir ses logiciels anti-virus et pare-feu, avec leurs mises à jour régulières, de faire des sauvegardes régulières et d'avoir une bonne connaissance par l'utilisateur des règles de sécurité.

Exercices

EXERCICE 1 – LA SÉCURITÉ DU SI D'UN SITE MARCHAND DE LOCATIONS

1. À quels types de risques s'expose-t-elle ?

Voici les principaux risques auxquels l'entreprise s'expose :

- les pirates (criminels ou non) ;
- le partage de fichiers sur les réseaux pair à pair (*peer to peer*) ;
- les logiciels malveillants (notamment virus, vers, chevaux de Troie) ;
- les attaques visant l'indisponibilité des serveurs ou ressources de l'entreprise (par déni de service ou déni de service distribué *via* des réseaux de robots) ;
- une amende en cas de divulgation des données personnelles des utilisateurs.

2. Quels sont les impacts potentiels de ces risques sur son activité ?

Les impacts potentiels de ces risques sur son activité sont :

- l'altération ou la destruction des données ;
- la mise en danger du système d'information de l'entreprise : indisponibilité des serveurs et/ou ressources en cas d'attaque par déni de service.

EXERCICE 2 – ESCROQUERIE PAR MESSAGERIE ÉLECTRONIQUE

1. De quoi s'agit-il ? Quel est le but recherché ?

Il s'agit d'une tentative d'usurpation d'identité par hameçonnage (*phishing*, en anglais) ciblant les clients de la banque.

L'hameçonnage consiste à leurrer un internaute pour l'inciter à communiquer ses données personnelles en se faisant passer pour un tiers de confiance. Cette technique frauduleuse se présente sous la forme d'un courrier électronique prétendument envoyé par la banque (logo). Sous prétexte d'améliorer la qualité du service, le message électronique demande au client de cliquer sur un lien hypertexte et de communiquer ses codes d'accès (identifiant et mot de passe) au service bancaire en ligne.

Le but recherché est de voler des informations personnelles ou professionnelles pour en faire un usage frauduleux.

2. Quels sont les risques ?

Les risques sont de fournir les renseignements demandés, c'est-à-dire des données personnelles (compte bancaire et mot de passe), qui seraient alors transmises directement aux pirates.

Les attaques par hameçonnage ciblent aussi bien les particuliers que les professionnels : en 2019, ce type d'attaque a constitué la première menace pour les entreprises (23 % des recherches d'assistance) et la troisième menace pour les particuliers (16 % des recherches d'assistance) d'après www.cybermalveillance.gouv.fr.

3. Quels sont les moyens de protection ?

L'usurpation d'identité par courrier électronique étant répandue, il faut prendre l'habitude de ne jamais donner suite à un message non sollicité demandant de fournir des données sensibles ou confidentielles, même s'il semble provenir d'un expéditeur connu. Il faut savoir aussi que les banques n'envoient jamais de demande de mise à jour par messagerie : celle-ci s'effectue toujours depuis un menu de l'application utilisée ou *via* un téléchargement sur le site Web sécurisé de la banque.

Il n'existe pas de parade absolue contre les tentatives d'hameçonnage, mais l'utilisation de logiciels pare-feu, antivirus, antispam, ainsi que le cryptage des données contribuent à une bonne protection technique.

Cependant, cela n'est pas suffisant et il convient d'adopter des bonnes pratiques concernant l'utilisation de la messagerie :

- Ne pas ouvrir les messages non familiers.
- Ne pas ouvrir les pièces jointes sans raison.
- Ne pas cliquer sur des liens hypertextes.
- Ne pas répondre aux messages douteux.

Dans ce cas précis, la tentative de *phishing* a été reçue par courriel : avant de cliquer sur le lien douteux, il faut positionner la souris sur ce lien (sans cliquer), ce qui permet d'afficher l'adresse vers laquelle il pointe réellement, afin d'en vérifier la vraisemblance.

Il est possible de signaler ce message douteux sur la plateforme Signal Spam (www.signal-spam.fr) qui, en partenariat avec les autorités publiques et la CNIL, pourra identifier et éventuellement lancer une enquête et sanctionner (voir les infractions encourues sur le site www.cybermalveillance.gouv.fr).

Il est possible de signaler l'adresse de site d'hameçonnage à Phishing initiative (www.phishing-initiative.fr), qui en fermera l'accès.

EXERCICE 3 – INCIDENTS DE SÉCURITÉ DANS LA SOCIÉTÉ DUBRULLE

1. Identifier les principaux risques répertoriés dans ces tickets d'incidents.

Ticket d'incident n° 1	Ticket d'incident n° 2
Le serveur de messagerie est saturé par une multitude de SPAMS.	En télétravail à domicile, un salarié a utilisé une clé USB sur son ordinateur portable. Depuis, il assiste à une ouverture intempestive de fenêtres sur son écran.
Réponse : une attaque par déni de service provoquée par une multitude de SPAMS a pour conséquence de diminuer la disponibilité du serveur de messagerie. Il y a un risque de perte de chiffre d'affaires pour l'entreprise.	Réponse : un cheval de Troie a permis l'intrusion de pirates sur l'ordinateur portable. Il y a un risque pour les données stockées sur celui-ci (copie, blocage, suppression) et de prise de contrôle à distance par des hackers.

Ticket d'incident n° 3 Le gestionnaire de paie a oublié de verrouiller son poste de travail lors de sa pause déjeuner. Réponse : la confidentialité des données n'a pas été respectée. Il y a un risque de communication des données sensibles des salariés (données à caractère personnel, données portant sur la rémunération, etc.).	Ticket d'incident n° 4 Impossible d'accéder au PGI Sage Ligne 100 suite à l'oubli du mot de passe après la période des congés d'été. Réponse : l'accès au réseau est impossible. Cette indisponibilité empêche le salarié de travailler. Il y a un risque de perte de productivité.

2. Quels sont les moyens de protection pour chaque ticket d'incident ?

Ticket d'incident n° 1 Le serveur de messagerie est saturé par une multitude de SPAMS. Réponse : le responsable du SI peut paramétrer une alerte dans un premier temps pour éviter la saturation du serveur de messagerie. Une autre solution consiste à dupliquer ce serveur pour assurer sa disponibilité.	Ticket d'incident n° 2 En télétravail à domicile, un salarié a utilisé une clé USB sur son ordinateur portable. Depuis, il assiste à une ouverture intempestive de fenêtres sur son écran. Réponse : un anti-virus adapté permettra de détecter le ou les programmes malveillants et de les détruire. En attendant, l'ordinateur infecté doit être isolé du réseau de l'entreprise.
Ticket d'incident n° 3 Un salarié a oublié de verrouiller son poste de travail lors de sa pause déjeuner. Réponse : l'utilisateur doit être sensibilisé à la politique de sécurité en vigueur dans l'entreprise, notamment au travers de la charte informatique et/ou par des actions de formation.	Ticket d'incident n° 4 Impossible d'accéder au PGI Sage Ligne 100 suite à l'oubli du mot de passe après la période des congés d'été. Réponse : l'utilisateur doit être sensibilisé à la politique de sécurité en vigueur dans l'entreprise, notamment au travers de la charte informatique et/ou par des actions de formation.

3. Comment vont être traités ces tickets d'incidents ?

En référence à la norme ITIL (bibliothèque pour l'infrastructure des technologies de l'information), deux critères permettent de fixer le degré de priorité d'un incident :

1. l'impact sur l'entreprise (fréquence, gravité, criticité sur l'activité) ;
2. l'urgence à trouver une solution.

Cas de synthèse

PRENDRE EN COMPTE LA DIMENSION HUMAINE DANS LA GESTION DES RISQUES

Mission 1 :

1.1. En cas d'attaque virale, quelles mesures doivent être mises en œuvre pour favoriser la continuité de l'activité ?

Pour favoriser la continuité de l'activité :

- d'un point de vue technique, l'infrastructure informatique doit être axée sur la tolérance de pannes et le rétablissement. Elle comprendra des composants matériels, logiciels et d'alimentation redondants visant à réduire les temps d'arrêt, des systèmes conçus pour récupérer rapidement d'un sinistre et des outils permettant aux utilisateurs de détecter les défaillances dans un environnement comprenant de multiples composants.
- du point de vue organisationnel, des plans de secours (plan de reprise après sinistre pour l'aspect technique et plan de continuité des activités pour l'aspect commercial), incluant les plateformes Web et mobile, permettront de faire face à tout type d'incident.

1.2. Quel est l'intérêt de faire des sauvegardes incrémentales ?

Une sauvegarde incrémentale permet de sauvegarder des données qui ont été modifiées ou ajoutées depuis la dernière sauvegarde. L'intérêt d'une sauvegarde incrémentale est qu'elle est plus rapide qu'une sauvegarde totale, puisque la sauvegarde concerne uniquement les derniers ajouts/modifications de fichiers entre deux sauvegardes.

1.3. Modifiez le cahier des charges pour prendre en compte les besoins exprimés par l'administrateur réseau

Extrait du cahier des charges à modifier

Antivirus

Le parc informatique est équipé d'un logiciel antivirus qui garantit une protection spécifique contre les virus de type « *ransomware* » et qui est géré de manière centralisée sur le serveur. Cette configuration permet une mise à jour automatique de l'antivirus pour tout le parc informatique, nomade ou non.

Sauvegarde

Un plan de sauvegarde performant combinant sauvegardes totales et incrémentales a été mis en place suite à l'élaboration du plan de continuité d'activité (PCA). Cette solution de sauvegarde repose sur la création de partages sur des serveurs de fichiers et sur des machines virtuelles de type VMware offrant :

- une restauration rapide et efficace des données ;
- des fonctionnalités avancées de réplication.

Organisation

Chaque salarié du service commercial est affecté à un poste de travail avec un matériel informatique relié au réseau. Il est sensibilisé aux bonnes pratiques numériques au travers de la

charte informatique affichée en salle de pause et grâce à des formations régulières. Les incidents doivent être signalés exclusivement *via* l'application GPLI.

Mission 2 :

2.1. Identifiez les principaux avantages du recours à une solution de gestions des tickets d'incidents.

Les principaux avantages sont :

- une centralisation des incidents, qui permet d'obtenir une base de connaissances sur les incidents les plus fréquents ;
- un seul outil basé sur une application Web de type GPLI pour l'assistance aux utilisateurs ;
- un gain de temps sur la résolution des incidents grâce à la base de connaissances ;
- la possibilité de documenter les utilisateurs grâce à une FAQ (foire aux questions) ;
- une procédure simple à appliquer ;
- un suivi efficace des résolutions d'incidents.

2.2. Rédigez les conseils applicables par les utilisateurs au choix du mot de passe, pour qu'ils soient ajoutés à la charte informatique.

Utilisez un mot de passe unique qui n'a pas de lien avec vous (évitez votre date de naissance ou le prénom de vos enfants, par exemple) et renouvelez-le fréquemment. Celui-ci doit comporter des lettres et des chiffres, et mesurer au moins 8 caractères.