Page 12

1. Nom, prénom, adresse, courriel.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Description** | **Référence** | **Finalité** | **Catégorie de DCP** | **Catégorie de personnes** | **Destinataire** |
| Enregistrement | OP-01 | Preuve de l’appel | Vie personnelle | Prospect | Client et service interne CentreCall |
| Collecte des réponses | OP-02 | Enregistrement des réponses | Vie personnelle, infos d’identité | " | " |
| Vérification de l’enregistrement | OP-03 | Vérification des réponses | " | " | " |
| Traitement des données | OP-04 | Utilisation pour synthèse étude de marché | " | " | " |

1. Non (cf. doc 2)

4. Pb : dates parfois mal renseignées en BD, et problème de cohérence entre ce qui est dit et ce qui est reçu en BD

Page 16 :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Source** | **Type** | **Bien support** | **Vraisemblance** | **Confidentialité** | **Disponibilité** | **Intégrité** |
| Attaquant extérieur | Espionnage | Ordinateur de l’opérateur | 2 | L’authentification n’est plus assurée aux seules personnes habilitées |  |  |
| Attaquant interne | Sabotage/Espionnage | Base de données | 4 | X | X | X |
| Attaquant interne | Humaine | Ordinateur de l’opérateur | 2 | X |  |  |
| Attaquant extérieur | Déstabilisation | Serveur de base de données | 3 |  |  | X |
| Attaquant extérieur | Sabotage | Serveur de base de données | 4 |  | X | X |

|  |  |  |
| --- | --- | --- |
| Scénario 1 | Usurpation d’identité | 3 - Les données confidentielles peuvent être exploitées par une entité malv. |
| Scénario 2 | Suppression/vol de données | 3 – Les données peuvent être modifiées, supprimées ou transmises. |
| Scénario 3 | Consultation de données | 2 |
| Scénario 4 | Altération de données | 3 |
| Scénario 5 | Arrêt du serveur BD | 4 – Impossibilité de travailler |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Traitement des inscriptions | Arrêt du serveur de la base de données |
|  | Exploitation des données confidentielles par une entité malveillante | Scénario 4 | Données modifiées, supprimées ou transmises à une entité extérieure. |
|  | Scénario 3 |  |  |
|  |  |  |  |

5.

Mme AZRI,

Votre système d’informations présente plusieurs vulnérabilités qui peuvent avoir un impact sur les missions de votre entreprise ou des impacts juridiques, et nécessite une intervention afin de renforcer la sécurité de vos données et de vos outils informatiques. Il nécessite l’installation de mécanismes d’authentification et de traçabilité. Par exemple, il serait essentiel de mettre en place un mécanisme de connexion qui donnerait des droits adaptés à la personne qui se connecte. Ou encore mettre en place des protocoles de chiffrements afin de garantir l’intégrité de vos données.

1. 5 risques identifiés
2. Donner les sources des menaces : extérieure ou intérieure (salarié, etc…)
3. Donner les types de menaces
4. Évaluation de la vraisemblance : la + et la –
5. Évaluation de la gravité
6. 3 risques majeurs (R2, R4 et R5) doivent être corrigés au plus vite.
   1. R2 -> Utilisation d’un logiciel de traçabilité au niveau logiciel BD ou en accès physique à un bureau
   2. R4 -> Installation d’un pare-feu pour limiter les attaques externes
   3. R5 -> Bien vérifier les sauvegardes à intervalles réguliers

p.29

1. b  
2. b et c  
3. b  
4. c  
5. b  
6. c  
7. b  
8. c  
9. b  
10. a et b

P32.

6.

|  |  |  |  |
| --- | --- | --- | --- |
| Scénarios | Sécurité | Sûreté | Justifications |
| L’ensemble des serveurs est hors-service à cause d’une inondation du local technique. |  | X | L’incident est survenu sans être causé par qui que ce soit. Ce n’est donc pas un acte malveillant. |
| Les données d’un hôpital sont illisibles à la suite d’une attaque *ransomware* | X |  | L’acte a été orchestré par un attaquant avec une volonté de nuire. |
| L’apparence du site vitrine d’une entreprise est modifiée pendant un week-end par des personnes malveillantes | X |  | « Personnes malveillantes » |
| Une surcharge électrique temporaire due à des travaux réalisés dans les bâtiments de la société provoque une panne des routeurs. |  | X | L’incident est survenu sans être causé par qui que ce soit. Ce n’est donc pas un acte malveillant. |

7.

|  |  |  |
| --- | --- | --- |
| Données | Caractère personnel | Justification |
| Le nom de l’enseigne Carrefour | Non | Pas personnel |
| L’adresse courriel professionnelle d’un directeur des services informatiques | Non | Adresse pro et publique |
| Une photo postée sur un réseau social | Oui et Non | Dépend compte public ou privé |
| Une vidéo de présentation de son parcours professionnel envoyée à une entreprise dans le cadre d’un recrutement | Oui |  |
| Les coordonnées GPS de localisation d’un smartphone | Oui | Permet de localiser une personne |
| Le groupe sanguin d’un patient stocké sur le serveur de base de données de son médecin | Oui |  |
| Les enregistrements de vidéosurveillance d’un datacenter | Oui |  |
| Le numéro d’enregistrement au registre du commerce et des sociétés d’une entreprise | Non | Concerne une entreprise |
| Le numéro de sécurité sociale d’un employé saisi sur sa fiche d’embauche | Oui | Unique, donc permet d’identifier |

p. 34

1. Date de conservation des données et liste des droits non précisés

2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Finalité du traitement | Base légale | Durée de conservation en base opérationnelle | Archivage | Observations |
| Réalisation d’études de marché | Contrat | 5 ans à compter de la dernière activité | 5 à 10 ans | Les données sont collectées lors du processus d’entretien téléphonique |
| Externalisation de l’accueil téléphonique | Contrat | 5 ans à compter de la dernière activité | 5 à 10 ans | Certaines DCP peuvent être fournies par des organisations clientes afin de faciliter l’externalisation de l’accueil téléphonique |
| Prévention de la fraude | Intérêt légitime | 3 ans à compter de l’inscription sur une liste d’alerte | 2 ans | Certaines données peuvent être collectées et conservées afin de vérifier l’identité réelle de la personne interrogée |
| Publicité ciblée ; profilage publicitaire | Consentement | 13 mois à compter du dépôt des cookies publicitaires | Pas d’archivage | Les cookies publicitaires sont accessibles dans le gestionnaire de cookies de la page d’information « cookies ». À tout moment, l’opposition au profilage publicitaire peut être demandée auprès de nos services |

1. "Bonjour monsieur,

Pour exercer votre droit à l’oubli, merci de nous en faire la demande soit par courrier soit par mail."

(Nique ta race pour le au revoir salope)

1. "Bonjour monsieur,

Afin de remédier à ce manquement ; nous envisageons de mettre en place le pare-feu StormShield SN510, qui inclut notamment un système de prévention d’intrusion."

(Tj pareil)

p. 38

1. Outil de sécurisation des salariés, c’est obligatoire

3. Réunion de présentation de la charte, affichage dans les bureaux

4. Diminution des coûts de stockage

p. 47

1. b et c  
2. b  
3. c  
4. b  
5. a et c  
6. a  
7. c  
8. a, c et d

p. 49

1. Données collectées => respect du RGPD obligatoire

Les données sont stockées pour une durée indéterminée.  
Les responsables peuvent visualiser l’ensemble des données.

p. 52

1.2. Car le principe d’intégrité n’est pas respecté (FTP sans chiffrement)

1.3. Le traitement des inscriptions présente une combinaison de gravité maximale, dû aux dégâts potentiels, et de vraisemblance élevée, car l’exploitation de cette faille est très probable. Elle est répertoriée comme inacceptable.

La cartographie du document carte présente le traitement des inscriptions comme un niveau de risque inacceptable, parce que le niveau de gravité est à 4, le plus haut, car cela impliquerait des conséquences très importantes pour l’entreprise.

2.1. 1- Confidentialité

2- Respect du principe du droits des personnes (réversibilité des données) du RGPD

3- Respect de l’obligation d’information du RGPD

4- Respect du principe de droit à la notification du RGPD

2.3.

Monsieur,

………………….

-Process traitement des inscriptions des nouveaux clients -> vulnérabilités organisationnelles et technologiques de déceler.

- Suite analyse des risques vis-à-vis des vulnérabilités -> inacceptable par l’organisation

-Objectif des propositions ci-dessous -> ramené le risque lié au traitement à « acceptable »

-Pour cela on vous propose :

T : Connexion BD -> mettre des id et mdp != du FTP  
 T : Utiliser un protocole de transport des données chiffré : SFTP (TLS…)  
 O : Ne pas partager ses id de connexions entre les salariés  
 T : Gérer plus « finement » les privilèges sur les accès liés aux données personnelles

Cordialement,

………………….

Page 58 :

Défiguration : déphasage et défacement

1. Logo + url/adresse site + nom : identité déclarative
2. Pour protéger l’identité juridique de M@Banque

Page 61 :

4- Sécuriser mieux le pb pour améliorer e-réputation : rétablir image

Page 61 :

1. Outil pour tester sécurité site web : Google Safe Browsing, URL Void, Dubbed observatory (mozilla), Skipfish (google)

Page 67 :

Voir td

Page 75 :

1 - c

2 – a b c

3 - a

4 – a b

5 - b

6 - a

7 - b

8 – a d (peut-être b et c mais non)

9 - a

10 – b c

Page 76 :

1. Identité déclarative : nom de domaine visé soit le nom de domaine ou IDN qui est visé
2. DNS poisoning

Pirate envoie requête au dns de tradec dans l’idée de le redirigé vers un serveur non officiel -> nom de domaine ne pointe plus vers le bonne ip

Page 86 :

Commutateur : switch en Fr -> appareil relier différent matériel sur réseau

Rooter : Matériel fessant le lien entre 2 réseaux

2VLAM pour réseaux

1. Risque : mot de passe trop simple, coller sur ordinateur, utilisation clés USB, complexité du mot de passe, cliquer sur des spams avec des liens dedans
2. Imposer certaines contraintes sur les mots de passes -> base recommandations NSI p100, donc stratégies mot de passe+ identifiant, stocker mots de passe / identifiant dans un coffre-fort électronique pas de post-it, autorisé – refuser par feu
3. Repérer les spams : adresse émettrice, fautes syntaxe, pas cliquer sur les liens, objet mail, contenu, pub, tout ce qui est lié à l’urgence, traiter mail comme indésirable
4. Charte informatique – règlement intérieur cf biod, cop, chod

Ajout 4e partie (voir question 1 et 2) à la charte informatique : a.Authentification, b.Attention mail(spam…) c.Bonne pratique lié à la messagerie

Page 91 :

1. Problème : Antivirus Windows désactiver, Contrôle application et navigateur désactiver, Mise à jour automatique désactiver voir nom app dans livre (Windows Smart Screen, Windows defender…)
2. Pare-feu : Analyse flux entrant / sortant de la machine (bloquer ou pas selon configuration)

Filtre courrier indésirable : Empêcher spams d’arriver sur les boites mails de l’utilisateur

Windows Update : mettre à jour système + patch

Logiciel Anti espion : Détection application de pub qui récupère des données pour les transmettre aux entreprises

Bloqueur de fenêtre publicitaire intempestive : adblock par exemple

Antivirus : Analyse code programme machine avec la signature virus (bdd)

1. Voir q2
2. Tous utile mais existe extension
3. 1 qui bloque via blacklist et l’autre faut configurer nom de domaine + catégorie (les 2 ça dépend config -> doc pas précis)

Page 103 :

1 : a b

2 : b

3 : c

4 : a b

5 : a b c d

6 : a b c

7 : b

8 : c

9 : a b

10 : a

Page 104 :

1 : Pare feu -> service proxy

2 : BlackList -> url dans la config du proxy et la rendre interdite (mot clé url)

3 : Proxy peut bloquer des protocoles + mettre règles IP / url

4 : Proxy ne permet pas de se protéger contre les malwares : pas vérifier signature des applications sur le pc

Page 105 :

1 : Empêcher l’exécution des ports USB dans le BIOS (désactivation)

2 : Mettre un mot de passe pour rentrer dans le BIOS

3 : Windows update

4 : Installation correctif + patch pour empêcher des failles de sécurité (identifié ou non)

5 : Installer un antivirus

Attaque par dictionnaire : liste de mdp fuité d’une bdd

Cf Attaque par rainbow table

Flux RSS : actualiser informatique

Keypass : gestion mot de passe (+ centraliser mdp / plus simple / chiffrement mdp) (- mot de passe trouvé -> perte de tous les mots de passe / si suppression fichier kdb : perte de tous les mdp / pluggins à tester avant : compromettre)

Kerberos : protocole pour le login

Privilège : crud

Habilitation : ajout view que les 2

Page 108 :

1. Désactiver compte admin (flèche en bas) et le mettre en jivon

Tout le monde à les droits et Groupe appartient à un autre groupe

Le groupe partenaire va avoir tous les droits (héritage)

Stratégie : paramétrage à un groupe (ex : groupe admin -> fond écran rouge)

1. Tout le monde peut tout voir -> désactiver le groupe tout le monde / utilisateur (risque héritage)

VLAN : découpage réseau en sous réseau virtuel

1. Impossible de répondre (mais quasi pareil)
2. Mettre chaque poste dans un vlan différent (doc 5 -> ce à quoi il faut arriver)

Page 111 :

* 1

Document 1 :

La mise en place des privilèges à fonctionner

Document 2 :

L’installation ne se lance pas : il faut le mdp utilisateur : plus les droits admin (plus d’héritage)

* 2 : Activer les logs au niveau des abonnements sur son serveur d’administration
* 3 : Oui : différent vlan crée, ping 1 échoué : normal -> 2 vlan différents, ping 2 marche : peut communiquer

2 réseaux logique et indépendant, les paquets passe par la passerelle pour communiquer avec l’un ou avec l’autre

QCM page 127 :

1 - 1

2 - 1

3 – 1 et 2

4 – 1 et 2

5 - 3

6 - 1

7 – 1, 2 et 3

8 – 1 et 2

9 - 1

10 - 2 et 2

11 - 2

Page 128 :

1. Chaque participant aura son dossier personnel : fichier isolé et seul visible par la bonne personne, retirer participant du groupe administrateur, mdp différent
2. Désactiver compte admin du compte de base et en refaire un avec un mdp perso, avoir une machine dédiée à l’admin, ne pas laisser les mdp trainer, ne pas mettre le prénom / nom de famille pour le login et avoir un mdp fort (12 caractères, chiffres, lettres…)
3. Consulter pour tout le monde par exemple (privilège)

Virer le groupe ou laisser tout le monde en lecture : acl : gestion utilisateurs (1 avec update, 1 avec update, delete…) : affecter droit / privilège

1. Registre des incidents, déclarations cnil, obligationnel cas d’incident, mesure technique et organisationnelle au niveau des données

Page 138 :

1. Données archiver non chiffrer, tout le monde peut accéder à la salle archive (pas dans la salle pas accessible à tous), clé problématique : si oublie de la clé, pas suffisamment sécurisé et accessible via (login?) mdp cf battement de 5mins : pb lie à la confidentialite

Page 139 : Cf sauvegarde, archivage et stockage

1. 1 serveur
2. Pb lié à la confidentialité, obligation générale de sécurité des locaux et des systèmes d’information et données non affiché
   1. Confidentialité
   2. Imputabilité des données / Intégrité

Page 140 :

1. Service non dispo : partie thème non accessible : intégrité ; page modifier, informations clients visible + coordonnées visibles
2. Données récupérées pas traiter : injection sql utilisé sur les autres clients donc : oui
3. Côté humain : détresse, peur, colère, panique, stress

Côté financière : Perte argent

1. Article cf 1ere colonne p156 : conséquence juridique : 2 ans prison + 30k d’amende

Page 143 :

1. Vidéo protection non installé, absence de protection pour la tour, serveur archive et client sont dans la même salle, copie du serveur tous les 6 mois : trop espacé, détecteur de fumé et un extincteur dans la salle d’archive
2. Non : Libre-service + oublie + identification de la personne : il faut automatiser et assigner une personne
3. Lien d’accès pas en HTTPS : page non chiffré : problème sécurité car il y a une transaction : protection données (autre pas protection de données)
4. Même avec mdp complet : si page pas chiffré ça ne change rien : non

Injection :

OR 1 = 1 ; INSERT INTO… ;# »

Page 157 :

1. B et C
2. A et C
3. B et C
4. C
5. A et B
6. B et C
7. B
8. B
9. B et C : attaque dos
10. A et C

Page 162 :

1. Serveur unique qui collecte les logs : centralisation des journaux

Redondance du serveur de collecte : 2 serv si pb

Action écrit dans les logs

Serveur d’action des logs du temps : avoir le temps précis des logs

VLAN dédié à la collecte des logs : sécurisé si embouteillage : log va arriver rapidement

* + - Bande passante dédié contrôle des logs QOS

Mise en place d’un serveur de consultation des logs : pour pouvoir les exploiter plus rapidement