COLLECTION BTS SIO

1RE ANNÉE

SIO

Services informatiques aux organisations

BLOC 3

CYBERSÉCURITÉ

des services informatiques

Livre du professeur

DELAGRAVE

COLLECTION BTS SIO

1RE ANNÉE

CYBERSÉCURITÉ

des services informatiques

Livre du professeur

Sous la direction de

François Saillard
IA-IPR d'économie-gestion,
président du jury BTS SIO,
académie d'Orléans-Tours

David Balny
IAN, agrégé d'économie-gestion,
membre du jury BTS SIO,
académie d'Orléans-Tours

Patrice Dignan
Agrégé d'économie-gestion, professeur et membre du jury en BTS SIO,
académie de Créteil

Jérôme Parra
Agrégé d'économie-gestion professeur et membre du jury en BTS SIO,
académie de Clermont-Ferrand

Jean-Pierre Souvanne
IAN, certifié d'économie-gestion, professeur en BTS SIO académie
de Strasbourg

DELAGRAVE

Sommaire

Thème 1 – Protéger les données à caractère personnel

Chapitre 1 – Identifier les risques liées aux données à caractère personnel p. 5

Chapitre 2 – Appliquer et diffuser la réglementation liée aux données à caractère personnel p. 21

Évaluation 1 p. 31

Thème 2 – Préserver l'identité numérique de l'organisation

Chapitre 3 – Préserver l'identité numérique de l'organisation p. 33

Évaluation 2 p. 45

Thème 3 – Sécuriser les équipements et les usages des utilisateurs

Chapitre 4 – Informer les utilisateurs et mettre en œuvre les défenses appropriées p. 47

Chapitre 5 – Sécuriser l'accès aux ressources et vérifier l'efficacité p. 57

Évaluation 3 p. 65

Thème 4 – Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

Chapitre 6 – Intégrer les enjeux liés aux cyberattaques et à l'obligation de protection des données p. 67

Chapitre 7 – Archiver et protéger les données et les preuves numériques p. 79

Évaluation 4 p. 89

Entraînement à l'épreuve E6 p. 81

Chapitre 1
Identifier les risques liés aux données à caractère personnel

Missions professionnelles

1 Recenser les traitements sur les données à caractère personnel, p. 12

1. Identifiez les données à caractère personnel parmi celles recueillies lors de la réalisation d'une étude de marché. Justifiez votre réponse.

La CNIL définit une donnée à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable ».
Au regard de cette définition, parmi les données recueillies lors de la réalisation d'une étude de marché (document 1), celles à caractère personnel sont : le nom, le prénom l'adresse complète et l'adresse courriel de la personne interrogée.

2. Analysez la conformité de la situation décrite avec les directives de la CNIL.

CentreCall répond seulement au premier point mentionné dans l'article de la CNIL : l'objectif de l'enregistrement de la conversation est précisé par l'opérateur.
Par contre les obligations suivantes ne sont pas respectées envers les personnes interrogées :

- qui sont les destinataires des écoutes ou enregistrements (service de formation, service client, etc.) ;
- l'information sur le droit d'opposition ;
- l'information sur le droit d'accès aux enregistrements.

3. Complétez le tableau de recensement des opérations réalisées lors d'une étude de marché chez CentreCall.

Description de l'opération	Référence	Finalité de l'opération	Catégories de données personnelles concernées	Catégories de personnes concernées	Destinataires
Enregistrement d'un appel téléphonique	OP-01	Preuve de l'appel	Vie personnelle	Prospect	Client et service interne de CentreCall

Collecte et sauvegarde des réponses au questionnaire	OP-02	Sauvegarde pour traitements ultérieurs	Identité, données d'identification, vie personnelle	Prospect	Client et services internes de CentreCall
Description de l'opération	**Référence**	**Finalité de l'opération**	**Catégories de données personnelles concernées**	**Catégories de personnes concernées**	**Destinataires**
Vérification et modifications des réponses suite à l'écoute de l'enregistrement audio.	OP-03	Vérification des réponses collectées	Identité, données d'identification, vie personnelle	Prospect	Client et services internes de CentreCall
Traitement des données collectées pour réaliser une synthèse par un logiciel	OP-04	Synthèse de l'étude de marché pour le client	Identité, données d'identification, vie personnelle	Prospect	Client et services internes de CentreCall

4. Repérez les difficultés rencontrées avec la nouvelle application. Précisez en quoi elles contribuent à affaiblir la protection des données à caractère personnel.

Les plateformes des centres d'appel sont désormais capables de gérer les demandes en provenance de plusieurs canaux (site internet, courriel, sms, appel vidéo, etc.).
La variété des technologies et des supports de collecte de données implique des protocoles réseau et des formats de fichier différents (xml, Json, etc.) qui nécessitent différents traitements.
Le multicanal influence donc le traitement des données à caractère personnel pour les centres d'appel comme CentreCall.

Solution au Ticket n° 1 :

Une inversion de date est constatée suite à l'utilisation de formats de données différents.
C'est l'intégrité de la donnée qui est en jeu.
Les formats doivent être uniformisés pour toutes les données de type « date » quel que soit le canal utilisé pour collecter les données.

Solution au Ticket n° 2 :

Certaines données doivent être saisies par un opérateur, c'est le cas pour les données émanant des entretiens téléphoniques. Cette saisie peut entraîner des erreurs et toucher à l'intégrité de données.

2 Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel, p. 16

1. Identifiez, dans la description du contexte, les éléments permettant d'identifier les vulnérabilités liées au traitement des données à caractère personnel.

L'intérêt d'une potentielle attaque réside dans la nature même des données collectées et dans la finalité de traitement de ces dernières.
Pour CentreCall, certaines données sont à caractère personnel.
Le cycle de vie des données lié au traitement (document 2) décrit les différentes opérations réalisées et permet d'identifier celles plus ou moins vulnérables à une attaque.
La collecte des réponses chez CentreCall peut engendrer des vulnérabilités sur les données à caractère personnel (enregistrement audio et sauvegarde par un opérateur des données collectées).
La liste des supports des données mobilisés lors du processus (document 2) permet de reconnaître le plus vulnérable à une attaque.
La communication via le téléphone IP peut être écoutée. L'ordinateur de bureau utilisé par l'opérateur peut subir une panne ou être la cible d'une attaque.

2. Complétez le tableau d'analyse des scénarios de menaces présenté dans le document 4. Justifiez les niveaux de vraisemblance retenus pour chaque menace.

Source de menace	Type de menace	Bien support	Niveau de vraisemblance	Critères de sécurité		
				C	D	I
Scénario de menace lié au **risque 1** : attaquant extérieur	Espionnage	Ordinateur de l'opérateur	**2 : limité** (les données ne sont présentes que sur le serveur de base de données.)	X (L'authentification n'est plus limitée aux personnes habilitées)		
Scénario de menace lié au **risque 2** : salarié	Espionnage	Serveur de base de données	**4 : maximal** (techniquement, l'action est facile à mettre en œuvre.)		X Les données ne seront plus disponibles après la suppression	
Scénario de menace lié au **risque 3** : salarié	Menace non intentionnelle	Ordinateur de l'opérateur	**2 : limité** (la confidentialité est normalement assurée par l'authentification des opérateurs.)	X Le salarié n'est pas habilité à accéder aux données		

Source de menace	Type de menace	Bien support	Niveau de vraisemblance	Critères de sécurité		
				C	D	I
Scénario de menace lié au **risque 4** : attaquant extérieur	Déstabilisation	Serveur de base de données	**3 : important** (aucune protection du serveur de base de données depuis l'extérieur n'est mentionnée.)			X Une modification de données est constatée
Scénario de menace lié au **risque 5** : attaquant extérieur	Déstabilisation	Serveur de base de données	**3 : important** (idem que le scénario lié au risque 4.)		X L'attaque rend le serveur indisponible	

C : confidentialité – **D** : disponibilité – I : intégrité.

Mesures de la vraisemblance : **1** négligeable – **2** limitée – **3** importante – **4** maximale.

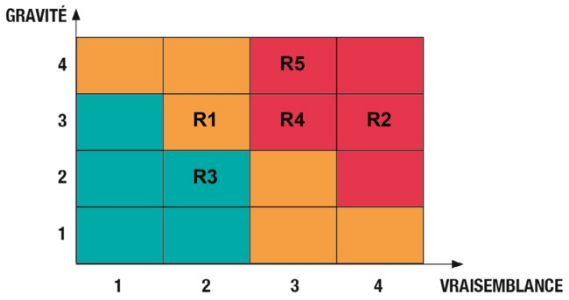
3. Retrouvez, pour chaque risque mentionné, l'événement redouté et son niveau de gravité estimé en complétant le document 5.

Exemple : scénario 1	Usurpation d'identité	**Niveau de gravité : 3 (important)** Les données confidentielles peuvent être exploitées par une entité malveillante.
Scénario 2	Suppression de données	**Niveau de gravité : 3 (important)** Certaines données ne seront plus accessibles.
Scénario 3	Consultation de données	**Niveau de gravité : 2 (limité)** La consultation de données se limite à un périmètre restreint.
Scénario 4	Altération de données	**Niveau de gravité : 3 (important)** La modification de données altère le résultat des études de marché.
Scénario 5	Arrêt du serveur de base de données	**Niveau de gravité : 4 (maximal)** Plus aucune donnée n'est accessible.

Mesures de la gravité : **1** négligeable – **2** limitée – **3** importante – **4** maximale.

4. Cartographiez les risques liés au traitement des données à caractère personnel par un schéma croisant les niveaux de vraisemblance et de gravité déterminés précédemment.

	Vraisemblance	Gravité
Risque 1	2	3
Risque 2	4	3
Risque 3	2	2
Risque 4	3	3
Risque 5	3	4



5. Rédigez une note de synthèse à l'intention de Mme AZRI pour l'informer des risques identifiés et de leur hiérarchisation. Cette note doit énumérer des propositions pour garantir la confidentialité et l'intégrité des données à caractère personnel dans le cadre du processus d'études de marché.

Mme AZRI,

Cinq risques ont été identifiés (voir document 4) avec des particularités propres à chacun.

Les **sources de menace** identifiées sont des attaques de personnes malveillantes situées à l'intérieur (salarié) ou à l'extérieur de notre société.

Les **types de menaces** sont l'espionnage au profit de concurrents ou la recherche de déstabilisation de notre processus d'étude de marché. Il est à noter une menace non intentionnelle correspondante à une erreur de manipulation d'un salarié.

Pour chaque menace, vous trouverez une **évaluation de sa vraisemblance**. Il semble que la récupération de données à caractère personnel suite au départ d'un salarié mécontent soit la menace la plus vraisemblable.

Une liste des événements redoutés permet de **mesurer leur niveau de gravité** suivant leurs impacts prévisibles sur les données à caractère personnel. Ainsi, l'arrêt du serveur de base de données apparaît comme l'événement redouté dont l'impact serait le plus préoccupant.

Une hiérarchisation nous permet d'identifier les **risques majeurs** suivants à surveiller :

- **Risque 2 :** suppression de données dans la base de données de CentreCall par un salarié mécontent dans l'objectif de les communiquer à un concurrent.
- **Risque 4 :** altération de données sur le serveur de base de données par un attaquant extérieur à l'organisation afin de déstabiliser les campagnes d'études de marché de CentreCall.
- **Risque 5 :** arrêt du serveur de base de données par une attaque extérieure en réalisant une multitude de requêtes.

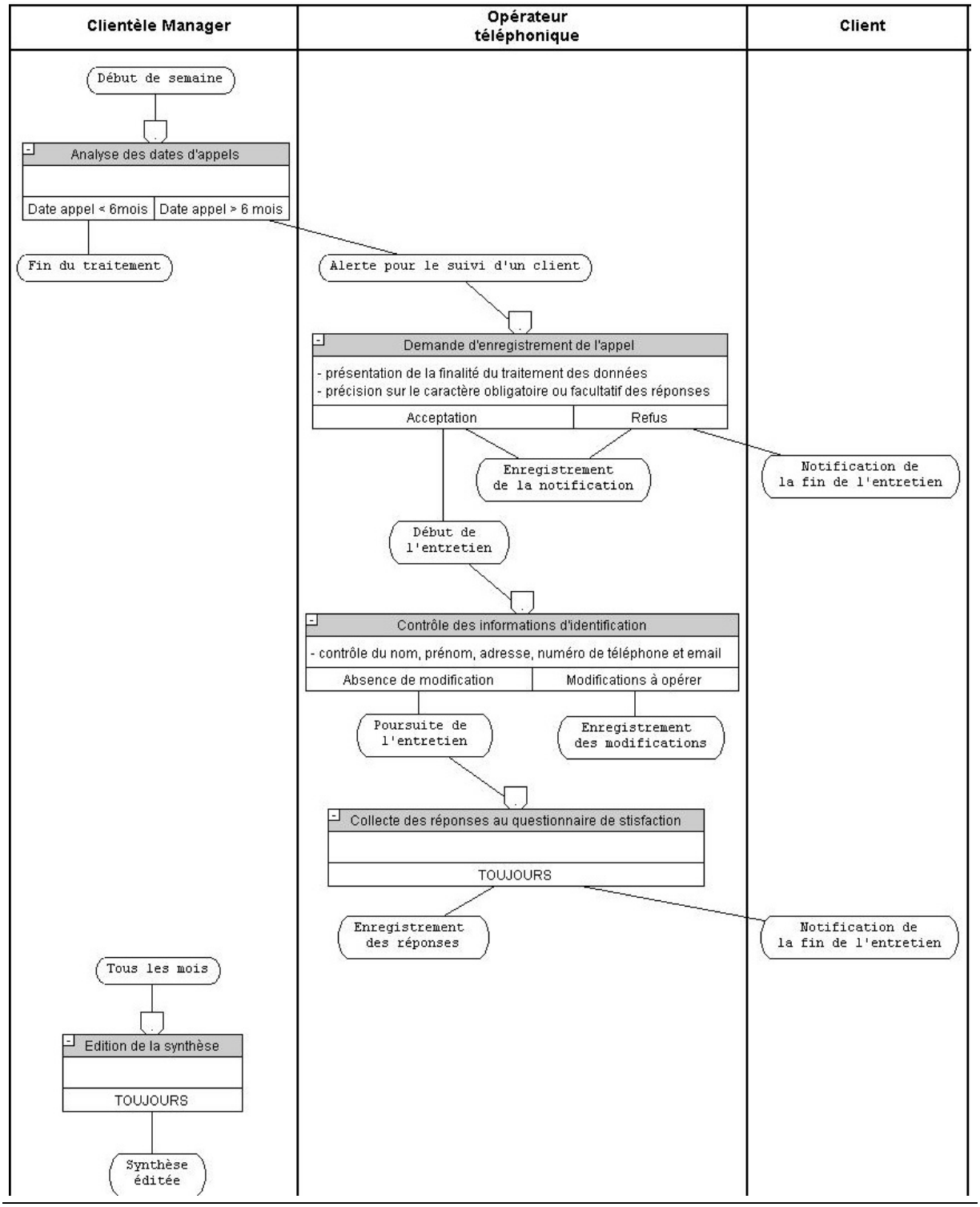
Le risque 2 correspond à une **impossibilité de garantir la confidentialité** des données, il peut être enrayé par une politique des mots de passe plus rigoureuse.

Le risque 4 peut mettre à mal l'**intégrité des données** stockées. Un pare-feu peut être une solution envisageable pour limiter les attaques extérieures.

Travaux en laboratoire informatique

1 Recenser les traitements sur les données à caractère personnel au sein de l'organisation, p. 19

1. Schématisez le processus de fidélisation en reprenant les éléments de l'entretien avec le directeur de la société ARTEMIS (document 1). Pour cela, vous utiliserez un logiciel adapté, par exemple JMOT.



2. Identifiez les données à caractère personnel liées au processus de fidélisation.

La CNIL définit une donnée à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise. »

Ainsi nous pouvons identifier dans le processus de fidélisation les données à caractère personnel suivantes : le nom, le prénom, l'adresse, le numéro de téléphone, le courriel et l'enregistrement audio de l'entretien.

3. Recensez les opérations réalisées sur les données à caractère personnel lors du processus de fidélisation.

5 opérations peuvent être recensées :

- l'analyse des dates d'appels ;
- la demande d'enregistrement de l'appel ;
- le contrôle des informations d'identification ;
- la collecte des réponses au questionnaire de satisfaction ;
- la préparation de la synthèse des échanges.

4. À l'aide des documents 2 et 3, complétez le registre numérique des activités de traitement (2e et 3e onglets du document numérique) en tenant compte des réponses apportées aux questions précédentes pour le processus de fidélisation.

💻Registre des activités de traitement : Ch1_Registre-traitement-CentreCall-Prof.ods

2 Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel, p. 21

ÉTAPE 1 Installation et analyse du paramétrage de l'outil

1. Téléchargez l'application PIA depuis le site de la CNIL :
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

2. Installez l'application pour ouvrir l'exemple de PIA.
L'application est compatible avec tous les systèmes d'exploitation. Un exemple est présenté afin de mieux comprendre les éléments attendus.

3. Décrivez les quatre phases représentées dans l'outil PIA qui correspondent au processus de l'analyse d'impact relative à la protection des données.

1. Le contexte
Cette phase permet d'obtenir une vision claire du (ou des) traitement(s) de données à caractère personnel considéré(s). Elle présente le traitement qui fait l'objet d'étude, le responsable de traitement, les données traitées, le processus du traitement et les supports de données mobilisés.

2. Les principes fondamentaux
Cette phase permet de bâtir le dispositif de conformité aux principes de protection de la vie privée. On vérifie les dispositions prises pour que les personnes concernées puissent exercer leurs droits en répondant à plusieurs questions.

- Sur la proportionnalité et la nécessité des données traitées
  - Les finalités du traitement sont-elles déterminées, explicites et légitimes ?
  - Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du traitement ?
  - Quelle est la durée de conservation des données ?
- Sur les mesures protectrices des droits
  - Comment les personnes sont-elles informées du traitement ?
  - Comment le consentement des personnes concernées est-il obtenu ?
  - Comment les personnes concernées peuvent-elles exercer leur droit d'accès et droit à la portabilité ?
  - Comment les personnes concernées peuvent-elles exercer leur droit de rectification et droit à l'effacement (droit à l'oubli) ?

3. Les risques
Cette phase aide à évaluer les risques sur la vie privée, compte tenu des mesures existantes ou prévues.

4. La validation
Cette dernière prépare la validation du PIA (*Privacy Impact Assessment*) ou l'analyse d'impact sur la protection des données.
Une cartographie des risques permet de les identifier et de les hiérarchiser. Un plan d'action peut être déterminé afin de limiter les impacts les plus importants.

ÉTAPE 2 Saisie des informations utiles pour le PIA

4. Saisissez les informations relatives à la délimitation du contexte étudié (mission 2, document 2, p. 22).

💻Registre des activités de traitement : Pia_Centrecall_Labo2_Q1-Q9.json

5. Retrouvez et enregistrez dans l'application PIA le dispositif mis en place permettant le respect des principes fondamentaux de protection de la vie privée (mission 2, document 2, p. 22).

💻Registre des activités de traitement : Pia_Centrecall_Labo2_Q1-Q9.json

6. Enregistrez dans l'application PIA les mesures existantes pour la protection de la vie privée (mission 2, document 2, p. 22).

💻Registre des activités de traitement : Pia_Centrecall_Labo2_Q1-Q9.json

7. Rapprochez chaque risque listé de l'une des trois catégories mentionnées dans l'application PIA.

Accès illégitime à des données	Modifications non désirées de données	Disparition de données
Risque 1, Risque 3	Risque 4	Risque 2

Le **risque 5** ne peut être listé dans l'une des catégories mentionnées dans l'application PIA. L'arrêt du serveur de base de données n'est pas un accès illégitime aux données, une modification non désirée des données ou une disparition de données.

8. Retrouvez et saisissez pour chaque catégorie de risque les éléments de réponse attendus.

💻Registre des activités de traitement : Pia_Centrecall_Labo2_Q1-Q9.json

ÉTAPE 3 Analyse des résultats de l'étude des risques

9. Générez la cartographie des risques dans l'application PIA.

💻Registre des activités de traitement : Pia_Centrecall_Labo2_Q1-Q9.json

10. Évaluez et commentez les informations d'un PIA saisies par l'un de vos camarades de classe en y apportant vos remarques sur l'application. Imprimez le plan d'action proposé et repérez les changements rendus visibles dans la cartographie.

💻Registre des activités de traitement : Pia_Centrecall_Labo2_Q10.json

Applications

1 QCM, p. 29

1. Quel indicateur permet de mesurer la probabilité de réalisation d'une menace ?

□ La gravité
☒ La vraisemblance
□ La nature de la menace

2. Le principe d'intégrité des données :

□ permet d'assurer une accessibilité sans interruption des données.
☒ peut être respecté par la mise en place d'un protocole de cryptage des données.
☒ s'assure que les données ne peuvent être modifiées pendant leur transfert, leur traitement ou leur stockage.

3. Quel terme est associé à la prévention des actes de malveillance ?

□ La sûreté
☒ La sécurité
□ La cybercriminalité

4. À quoi correspond une attaque par « point d'eau » (*wateringhole*) ?

□ L'usurpation d'identité d'une personne pour envoyer un message ciblé
□ L'action de rendre inaccessible un service par l'envoi d'une multitude de requêtes
☒ L'infection du site internet d'une organisation pour contaminer les ordinateurs des visiteurs du site et accéder au réseau de l'organisation

5. Les données à caractère personnel :

□ représentent seulement les données qui identifient directement une personne.
☒ sont composées de données qui peuvent identifier directement ou indirectement une personne.
□ peuvent correspondre aux coordonnées d'une organisation.

6. Quels sont les éléments qui permettent d'apporter la preuve d'un acte malveillant ?

□ Les seules conséquences de l'acte malveillant
□ L'acte malveillant en lui-même
☒ L'authentification, l'imputabilité et la traçabilité

7. À quoi correspond une attaque par « déni de service » ?

□ Les données sont cryptées et une demande de rançon est formulée.
☒ Un service est rendu inaccessible par l'envoi d'une multitude de requêtes.
□ L'usurpation d'identité

8. Un traitement de données :

□ correspond à la phase de collecte des données.
□ correspond à la phase d'enregistrement des données.
☒ englobe toutes les opérations de la collecte à la diffusion des données.

9. Un responsable de traitement doit :

□ traiter l'ensemble des données de l'organisation.
☒ faire respecter les droits

fondamentaux en matière de protection des données à caractère personnel.

□ rendre opérationnel l'ensemble des serveurs de bases de données.

10. Quels peuvent être les impacts des risques informatiques ?

☒ La perte de crédibilité dans les décisions stratégiques de l'organisation

☒ Des pertes financières

□ L'attraction de nouveaux clients

2 Analyser un PIA, p. 30

1. Importez le travail réalisé par Monsieur Grospire dans l'application PIA.

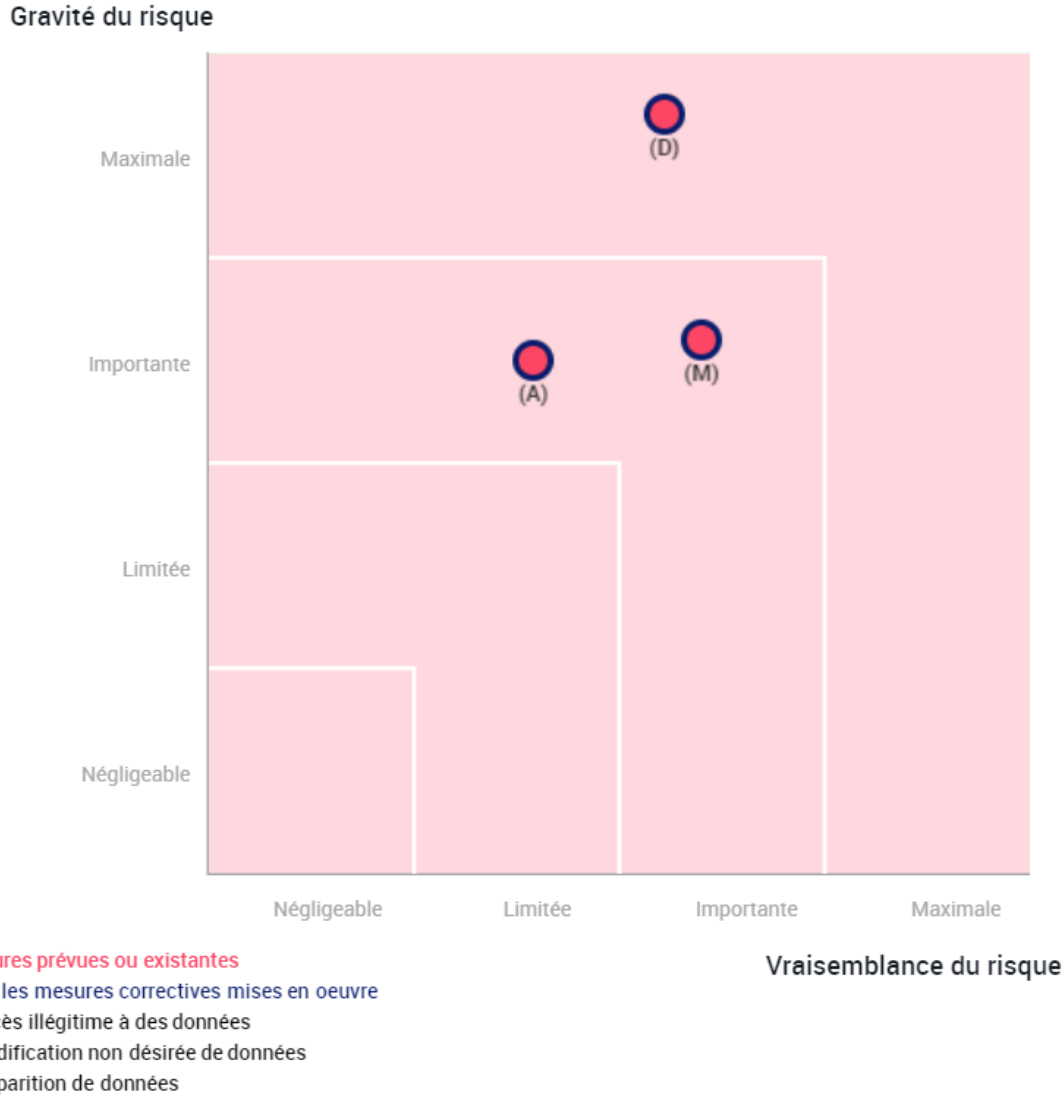
💻Registre des activités de traitement : Delagrave_Application2_Ch1_PIA_TESTOP.json

2. Évaluez les niveaux de gravité et de vraisemblance des trois risques principaux pouvant affecter les données à caractère personnel compte tenu des informations déjà saisies.

💻Registre des activités de traitement : : Pia_TESTOP_Application2_Q2.json

3. Affichez et commentez la cartographie des risques.

💻Registre des activités de traitement : : Pia_TESTOP_Application2_Q3.json

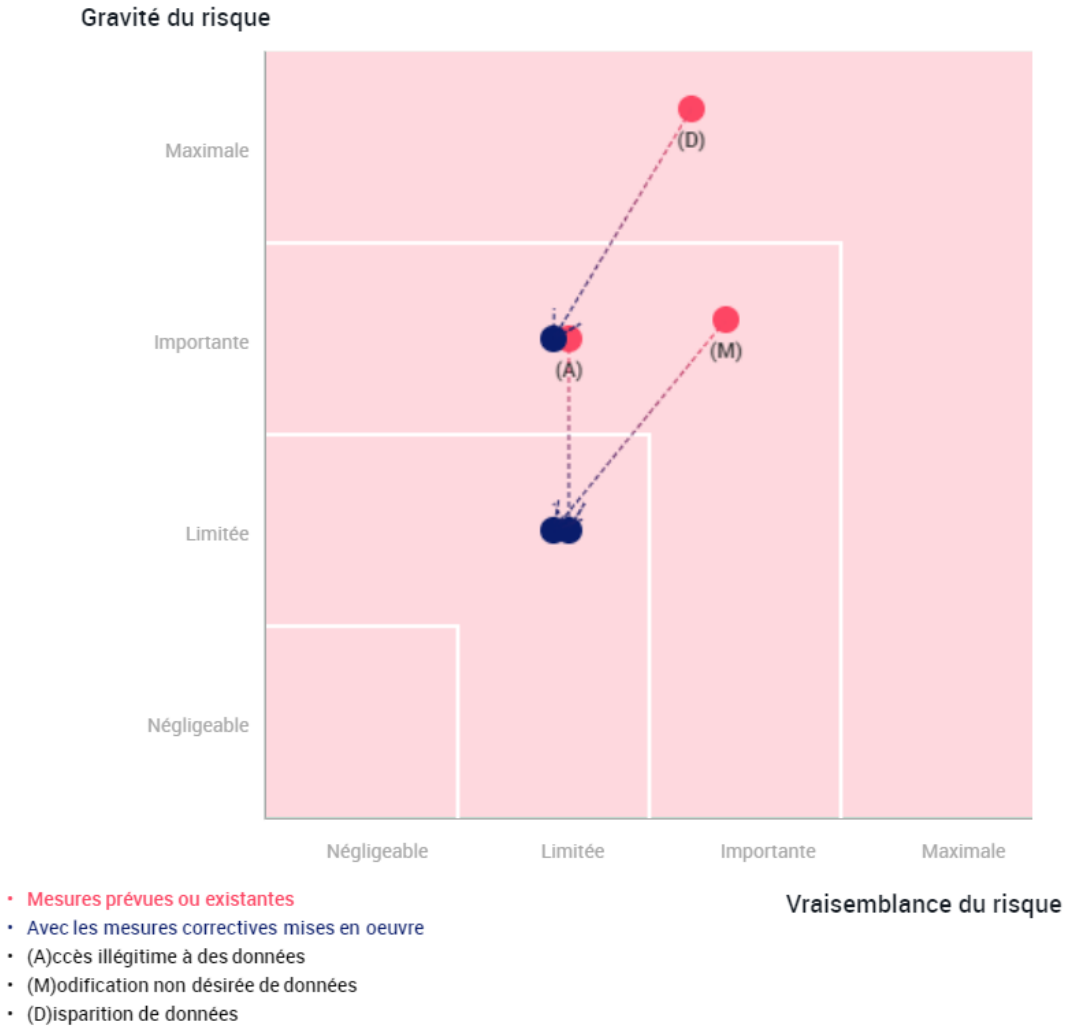


À la lecture de la cartographie des risques, il apparaît, dans un premier temps, que la gravité maximale est affectée à la perte de données personnelles concernant les salariés de l'organisation. C'est donc ce risque qu'il faut traiter en priorité.
Dans un second temps, ce sont les modifications de données du processus de recrutement qui sont le plus vraisemblables avec une gravité importante. Ce serait donc le deuxième risque à traiter.
Enfin le risque d'un accès illégitime aux données des salariés semble peu vraisemblable mais la gravité est importante. Ce sera ce dernier risque qu'il faudra traiter.

4. Évaluez les différents items en proposant, le cas échéant, des mesures correctives envisageables.

💻Registre des activités de traitement : : Pia_TESTOP_Application2_Q4.json

5. Commentez l'évolution de la cartographie des risques sur les données à caractère personnel.



Nous pouvons constater que les nouvelles mesures préconisées pourraient limiter les risques liés à l'accès illégitime, la modification ou encore la disparition de données.
Seul le risque lié à la disparition de données conserve une gravité importante malgré les propositions formulées.

3 Cartographier le traitement des données à caractère personnel, p. 30

1. Après avoir visionné la vidéo, expliquez en quoi consiste la cartographie des traitements des données personnelles et quels sont ses enjeux.

La cartographie des risques aide à identifier les risques en fonction des traitements réalisés sur les données. Le risque est en rapport avec la sensibilité et le lieu de stockage des données qui permettent d'évaluer sa vulnérabilité et sa gravité.

2. Pourquoi le registre des traitements des données à caractère personnel est-il une étape préalable à la cartographie des traitements ?

Le registre des données permet de visualiser quelles sont les données traitées par l'organisation, où elles se situent.
La cartographie des traitements doit favoriser la visualisation des risques sur les données personnelles, ces risques sont liés au lieu de stockage et aux traitements réalisés. Ces derniers éléments se retrouvent dans le registre des données.

4 Repérer l'utilisation des données à caractère personnel, p. 31

1. Précisez les conséquences de la saisie de données personnelles sur un formulaire d'inscription au site castorama.fr, à l'aide de l'annexe.

Les données personnelles saisies sur le formulaire d'inscription du site sont amenées à être communiquées à d'autres organisations (groupe Kingfisher, assureurs, organisations tiers). Ces organisations peuvent, par la suite, proposer des offres commerciales ciblées.

2. Expliquez si la seule lecture de cet extrait peut permettre d'affirmer que la confidentialité des données personnelles n'est pas assurée.

Nous ne pouvons pas affirmer avec ce seul extrait que la confidentialité des données est assurée ou non. Il faudrait que Castorama communique des informations sur les éléments organisationnels et techniques qui assurent cette sécurité.

5 Traitements et risques sur les données à caractère personnel, p. 31

1. Après avoir visionné la vidéo, repérez les différents moyens de collecte, stockage et diffusion des données à caractère personnel.

- **Moyens de collecte :** questionnaire en ligne, enregistrements vocal et vidéo, réseaux sociaux…
- **Moyens de stockage :** fichier, base de données.
- **Moyens de diffusion :** courriels, téléphone.

2. Quels sont les traitements des données à caractère personnel présentés ?

Les traitements des données à caractère personnel présentés sont : la gestion du personnel, le contrôle d'accès par badges, système de surveillance.

3. Listez les obligations légales rappelées dans la vidéo.

Les obligations légales rappelées dans la vidéo sont :

- définir la finalité du traitement ;
- limiter la collecte de données au strict nécessaire ;
- collecter des données pertinentes au regard de la finalité ;
- veiller à la suppression des données une fois le traitement réalisé ;
- assurer la sécurité et la confidentialité des données.

4. Indiquez les sanctions encourues par les entreprises en cas de non-respect de la sécurité des données à caractère personnel.

Les sanctions encourues par les entreprises en cas de non-respect de la sécurité des données à caractère personnel sont :

- 4 % du chiffre d'affaires d'un groupe et jusqu'à 20 millions d'euros en cas de violation des principes de sécurité des données personnelles.
- 2 % du chiffre d'affaires et jusqu'à 10 millions d'euros si la sécurité des données personnelles n'est pas adaptée.
- des peines d'emprisonnement jusqu'à 5 ans peuvent être prononcées avec publication des infractions.

6 Dissocier les notions de sécurité et de sûreté informatique, p. 32

Retrouvez, dans les scénarios proposés ci-dessous, ceux qui relèvent de la notion de sécurité et ceux qui relèvent de la notion de sûreté. Justifiez.

Scénarios	Sécurité	Sûreté	Justifications
L'ensemble des serveurs est hors-service à cause d'une inondation du local technique.	☐	☒	Ce n'est pas un acte de malveillance.
Les données d'un hôpital sont illisibles à la suite d'une attaque de type *ransomware*.	☒	☐	C'est un acte de malveillance.
L'apparence du site vitrine d'une entreprise est modifiée pendant un week-end par des personnes malveillantes.	☒	☐	C'est un acte de malveillance.
Une surcharge électrique temporaire due à des travaux réalisés dans les bâtiments de la société provoque une panne des routeurs.	☐	☒	Ce n'est pas un acte de malveillance.

7 Identifier les données à caractère personnel, p. 32

Recensez les données qui correspondent à la définition d'une donnée à caractère personnel. Justifiez.

Données	Caractère personnel	Justifications
Le nom de l'enseigne du magasin Carrefour	☐oui ☒non	Le nom de l'enseigne d'une organisation n'est pas considéré comme une donnée personnelle.
L'adresse courriel professionnelle d'un directeur des services informatiques	☐oui ☒non	Il s'agit de l'adresse courriel professionnelle et non personnelle donc ce n'est pas une donnée à caractère personnel.
Une photo postée sur un réseau social	☒oui ☒non	Tout dépend du caractère privé de la photo postée.
Une vidéo de présentation de son parcours professionnel envoyée à une entreprise dans le cadre d'un recrutement	☒oui ☐non	La vidéo permet d'identifier facilement la personne c'est donc une donnée à caractère personnel.
Les coordonnées GPS de localisation d'un smartphone	☒oui ☐non	Les coordonnées GPS permettent d'identifier la localisation d'une personne, c'est donc une donnée à caractère personnel.
Le groupe sanguin d'un patient stocké sur le serveur de base de données de son médecin	☒oui ☐non	Par définition, c'est une donnée à caractère personnel.
Les enregistrements de vidéosurveillance d'un *data center*	☒oui ☐non	Les images recueillies pendant la vidéosurveillance peuvent être des données à caractère personnel si elles permettent d'identifier une personne.
Le numéro d'enregistrement au registre du commerce et des sociétés d'une entreprise	☐oui ☒non	Le numéro d'enregistrement du commerce est une information rattachée à une organisation donc ce n'est pas une donnée à caractère personnel.
Le numéro de Sécurité sociale d'un salarié saisi sur sa fiche d'embauche	☒oui ☐non	Le numéro de Sécurité sociale d'un salarié permet de l'identifier c'est donc une donnée à caractère personnel.

Chapitre 2
Appliquer et diffuser la réglementation liée aux données à caractère personnel

Missions professionnelles

1 Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel, p. 34

1. Vérifiez la conformité de la charte de confidentialité de CentreCall avec les principes fondamentaux de la protection des données à caractère personnel de la CNIL.

Le principe de finalité	Dans le document 1, il est précisément mentionné les différentes finalités des traitements sur les données à caractère personnel : - la réalisation d'études de marché pour le compte de clients ; - l'externalisation de l'accueil téléphonique de clients ; - la sécurité de notre site ; - la personnalisation des publicités en ligne (publicité ciblée).
Le principe de proportionnalité et de pertinence	Les données collectées (nom, prénom, etc.) par CentreCall sont pertinentes au regard des finalités listées précédemment.
Le principe d'une durée de conservation limitée	Les durées de conservation des données sont limitées et proportionnelles aux finalités. Le document 2 présente les durées d'archivage relatives aux différents traitements réalisés. (Exemple : 5 à 10 ans pour les données collectées lors d'une étude de marché).
Le principe de sécurité et de confidentialité	CentreCall dispose d'un pare-feu certifié ANSSI qui assure le filtrage et la détection des tentatives d'intrusions. De plus l'ensemble des serveurs de données sont répliqués pour une restauration sécurisée et rapide. Les applications développées par CentreCall pour collecter et traiter les données à caractère personnel intègrent des dispositifs qui sécurisent les flux d'informations et évitent des actes malveillants qui viseraient les bases de données.
Les droits des personnes	Aucune information ne rappelle aux personnes concernées par la collecte de données comment exercer leurs droits (droits à la portabilité des données, à l'oubli et à la notification).

2. Retrouvez sur quelle base légale s'appuie la conservation des données à caractère personnel par CentreCall. Complétez le tableau puis justifiez votre réponse.

Finalité du traitement	Base légale	Durée de conservation en base opérationnelle	Archivage	Observations utiles
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 données à caractère personnel 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 colletées 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.

3. Répondez à la demande d'information formulée par une personne interrogée lors d'une étude de marché réalisée par CentreCall.

La réponse apportée par CentreCall doit rappeler à Maurice Bleuet qu'une simple demande écrite peut permettre d'exercer son droit à l'oubli (droit à l'effacement de ses données et au déréférencement).

4. Proposez une réponse argumentée au courrier de la CNIL, à l'aide des informations fournies par vos collègues.

Monsieur Bromont,
Suite à votre notification, nous avons acquis et paramétré un nouveau matériel palliant les vulnérabilités soulignées. Celui-ci intègre un système de prévention d'intrusion (ou IPS, *intrusion prevention system*) qui permet de prendre les mesures nécessaires en cas d'attaque. C'est un IDS (*intrusion detection system* ou système de détection d'intrusion) actif, puisqu'il détecte par un scan automatisé les ports ouverts et les bloque automatiquement.

5. Rédigez une note à destination de M^{me} Azri sur la conformité du contrat de sous-traitance au regard des obligations en matière de protection des données à caractère personnel du RGPD. Justifiez en vous appuyant sur les informations fournies par la société Osiris.

Madame Azri,

Le règlement général sur la Protection des données (RGPD) précise que les transferts de données à caractère personnel hors de l'UE doivent respecter plusieurs conditions, notamment que le pays tiers présente un niveau de protection adapté.

La société Osiris présente des garanties dans ce sens.

Elle travaille avec de nombreux partenaires européens et notre politique concernant la protection des données à caractère personnel est conforme aux exigences du RGPD.

Les lieux de stockage de données sont hautement protégés par un pare-feu et les flux de ces données sont isolés et sécurisés (chiffrement des données stockées, chiffrement des transmissions de données et traçabilité des opérations). Il est également précisé que le personnel est formé au respect des droits à la protection des données.

En conclusion, un contrat de sous-traitance avec la société OSIRIS – basée en Inde – est envisageable au regard des éléments mentionnés ci-dessus et de leur conformité avec la législation européenne.

2 Sensibiliser les utilisateurs à la protection des données à caractère personnel, p. 38

1. Précisez en quoi l'existence d'une charte informatique peut contraindre les utilisateurs du SI de CentreCall à être plus vigilants dans la protection des données à caractère personnel.

La charte informatique est un outil de sensibilisation des salariés à la protection des données à caractère personnel. Elle s'impose à eux et précise son domaine d'application, les conditions d'accès au réseau par les utilisateurs et les points de vigilance pour le respect de la confidentialité des informations. Comme indiqué dans le document 2, la charte informatique a la même valeur que le règlement intérieur.

2. Expliquez en quoi la publication de la charte informatique peut constituer un élément de sensibilisation des collaborateurs de CentreCall.

Une charte informatique est un élément d'organisation de la vie de l'entreprise : elle peut être le fruit d'une concertation. Elle doit être respectée par chaque salarié et donc avoir du sens pour tous. Aussi, sa rédaction est déjà une étape de sensibilisation puisqu'elle peut remettre en cause certains comportements. De plus, sa publication – par voie d'affichage ou autre – ne peut que mettre l'accent sur les responsabilités de chacun en matière de sécurité et insister sur le caractère obligatoire de la charte.

3. Proposez d'autres supports de communication qui pourraient être réalisés dans le cadre de cette campagne de sensibilisation.

Le sujet de la sécurité des données est un enjeu stratégique pour l'entreprise, pourtant il intéresse peu les collaborateurs, et les messages autour des bonnes pratiques sont souvent austères. Partant de ce constat, plusieurs supports peuvent être mobilisés pour susciter une prise de conscience des problèmes de sécurité et favoriser des discussions sur la cybersécurité entre les différents utilisateurs. Par exemple, une campagne de sensibilisation réalisée via des **films d'animation** et conçue sur le **modèle des séries TV** accompagnée de séquences pédagogiques. Dans un article rédigé par Stéphane Bellec pour le compte de BFMTV, Mathieu Benasar, manager pôle conseil chez Lexsi (sécurité IT) relève cinq méthodes pour sensibiliser les salariés à la sécurité :

1. Associez la direction générale à vos messages.
2. Dispensez des cours et des tests en ligne.
3. Simulez les dangers dans un jeu vidéo.
4. Faites témoigner des experts.
5. Mettez vos collaborateurs à l'épreuve.

(Cf. l'article complet : https://bfmbusiness.bfmtv.com/01-business-forum/cinq-methodes-pour-sensibiliser-vos-salaries-a-la-securite-597505.html)

4. Retrouvez comment CentreCall peut améliorer son fonctionnement grâce au RGPD.

Selon l'article présenté, le RGPD améliore le fonctionnement d'une organisation comme CentreCall pour plusieurs raisons.

- La mise en place du RGPD oblige CentreCall à se questionner sur les raisons et le type de données stockées. Elle peut ainsi limiter le volume de données stockées – notamment celles à caractère personnel qui ne sont pas ou peu utiles pour ses processus métiers.

- La diminution du volume de données et des failles de sécurité qui peuvent entraîner un arrêt de l'activité engendrent une diminution des coûts. Ces économies sont propices à investir davantage dans la sécurité.

Travaux en laboratoire informatique

Concevoir une journée de formation sur la protection des données à caractère personnel, p. 41

ÉTAPE 1 : Préparation du protocole de la formation

1. Définissez l'objectif principal de la formation et les objectifs intermédiaires, à partir du programme de la journée.

- **Objectif principal :** former les opérateurs téléphoniques à la protection des données à caractère personnel.
- **Objectifs intermédiaires :**
  - sensibiliser les opérateurs téléphoniques à la protection des données à caractère personnel ;
  - présenter la politique de protection des données personnelles de CentreCall.

2. Choisissez l'approche pédagogique la plus appropriée à chaque atelier. Justifiez.

- **L'atelier 1** a pour objectif la sensibilisation des opérateurs téléphoniques à la protection des données personnelles. Il semble que l'approche participative soit la mieux adaptée pour intégrer les enjeux de cette démarche de protection.
- **L'atelier 2** doit être une présentation de la politique de protection des données personnelles de CentreCall. Il ne s'agit pas ici de construire cette politique avec les salariés mais de leur communiquer le cadre réglementaire en matière de sécurité des données. La communication relève plutôt d'une approche démonstrative de la part des formateurs.

ÉTAPE 2 : Préparation des supports de l'atelier 1

3. Testez le scénario d'immersion des opérateurs téléphoniques en respectant le cahier des charges présenté dans le document 3.

💻Importation de la machine virtuelle : Chapitre 2-Laboratoire-Delagrave.ova

Le scénario sensibilise les étudiants au fait que la première faille de sécurité repose sur l'humain.

Ce scénario permet également de mobiliser plusieurs compétences transversales comme l'attribution de droits des utilisateurs sur une base de données, l'utilisation d'un environnement de machines virtuelles et les principes de base de l'adressage réseau.

4. Essayez de supprimer le contenu de la table « clients ». Qui sera responsable de l'incident aux yeux de l'équipe de sécurité du réseau ?

L'opérateur1 peut maintenant supprimer un enregistrement de la table « clients » puisqu'il dispose de la session de l'utilisateur callmanager1 avec les droits de suppression associés.
Le responsable aux yeux de l'équipe de sécurité du réseau est le callmanager1.

5. Critiquez le support de sensibilisation présenté dans le document 4, puis réalisez votre propre version en utilisant un logiciel adapté (par exemple canva.com). Le document sera au format d'une feuille A4.

Deux critiques peuvent être apportées au support de sensibilisation :

- sur la forme : il apparaît peu enclin à attirer le regard des salariés ;
- sur le fond : le message est austère et direct. Il n'engage pas la réflexion et la sensibilisation des salariés. Ils peuvent avoir des difficultés à intégrer le sens du message.

Toutes propositions de créations de supports de la part des étudiants permettant d'éluder les deux critiques citées ci-dessus peuvent être valorisées.
Exemple : création d'un document sur le ton de l'humour ou présentant des conséquences du non-respect de la règle de confidentialité.

ÉTAPE 3 : Préparation des supports de l'atelier 2

6. Élaborez un diaporama présentant les points essentiels de la politique de protection des données à caractère personnel de CentreCall.

Les étudiants doivent reprendre les principaux éléments du contexte de CentreCall pour concevoir leur proposition de diaporama (document 1, p. 35 et document 1, p. 39).
Pour optimiser la présentation du diaporama, il existe des préconisations à respecter :
« L'objectif est d'insérer un minimum de texte. Pour que le diaporama reste un support visuel, chaque diapositive doit comporter au maximum trente mots, soit trois à quatre phrases.
Le message doit être clair, simple et lisible.
Guy Kawasaki préconise, dans son ouvrage *L'art de se lancer*, la règle des « 10/20/30 » :

- **10** pour le nombre de diapos de façon à rester concis ;
- **20** pour les 20 minutes que doit durer une présentation, avant que l'intérêt de l'auditoire ne faiblisse ;
- **30** pour le corps de la police à utiliser dans une diapo.

La réflexion sur le design et la composition graphique que l'on souhaite appliquer à la présentation intervient au début et non à la fin. Elle dépend des idées à véhiculer, à organiser, à clarifier :

- disposition : contraste, sens de la lecture, hiérarchie, position ;
- éléments visuels : fond, couleur, texte, image.

Par ailleurs, il est recommandé de laisser 50 % de la diapositive vierge : cela permet de mettre en relief davantage les informations et images affichées.
Pour choisir la couleur à utiliser dans la diapositive ou des éléments, il faut prendre en compte la charte graphique ou les couleurs du logo de l'entreprise.
Il est fortement recommandé :

- de ne pas utiliser plus de deux polices différentes ;
- homogénéiser la taille de police d'une diapositive à l'autre, sauf pour différencier volontairement un message par rapport à un autre.

L'image a une triple fonction, c'est pour cela qu'il faut faire attention à la netteté et la clarté de l'image :

- illustrer efficacement le propos ;
- favoriser la mémorisation du message ;
- libérer l'orateur de son écran. »

Source : https://fr.wikiversity.org/wiki/Diaporamas/Règles_d'utilisation

ÉTAPE 4 : Évaluation et suivi de la formation

7. Choisissez un outil d'évaluation adapté et listez cinq questions qui pourraient être posées en fin d'intervention pour vérifier les acquis des nouveaux opérateurs téléphoniques.

Toute proposition d'outil d'évaluation doit être argumentée et on attend, au minimum, que l'un des deux outils mentionnés dans le document 6, p. 44, soit mobilisé.
Les questions doivent permettre de mesurer l'impact de la formation et les modifications à y apporter.
Elles doivent porter sur le contenu de la politique de sécurité de CentreCall mais également sur les propositions de supports et d'approche pédagogique arrêtés.
Exemples :

- Sur le contenu de la politique de sécurité : « Quelle est la condition préalable à respecter avant l'utilisation des ressources informatiques de CentreCall ? »
- Sur les éléments utilisés pour la formation elle-même : « Les supports de formation proposés vous ont-ils aidés à mieux comprendre le sens des règles de la politique de sécurité de CentreCall ? »

Applications

1 QCM, p. 47

1. Quelles sont les données qui peuvent être considérées à caractère personnel ?

□ Le nom d'une entreprise cliente

☒ L'adresse d'un client saisie à l'aide d'un formulaire sur le site vitrine

☒ La vidéo de surveillance du portail d'entrée de l'entreprise

2. Le droit à l'oubli :

□ assure à toute personne le droit de récupérer les données collectées par une entreprise pour les transférer à une autre.

☒ assure à toute personne la possibilité de demander que ses données soient effacées.

□ permet à une personne d'être informée de la vulnérabilité de ses données collectées par une entreprise.

3. La création d'un registre des activités de traitements est obligatoire pour :

□ les organisations de plus de 50 salariés.

□ les organisations de plus de 150 salariés.

☒ les organisations de plus de 250 salariés.

4. Quel est le rôle du délégué à la protection des données ?

□ Mettre en place une politique de sécurité du SI

☒ Mettre en œuvre la conformité au RGPD

□ Recruter les salariés de la DSI et assurer leurs formations

5. L'organisme collectant des données à caractère personnel doit informer les individus concernés par la collecte afin de respecter :

☒ le principe de finalité.

□ le principe de sécurité et de confidentialité.

□ les droits des personnes.

6. Dans le cas d'une violation de la sécurité des données à caractère personnel, le responsable du traitement doit alerter les personnes concernées :

☒ selon le droit à notification.

□ selon le droit à l'oubli.

□ selon le droit à la portabilité des données.

7. Quels sont les rôles de la CNIL ?

□ C'est une autorité sous la responsabilité de l'État dont le rôle est de surveiller les informations qui circulent sur Internet.

☒ C'est une autorité indépendante qui veille à ce que l'informatique ne porte pas atteinte aux libertés des citoyens.

☒ C'est une autorité qui veille au respect de l'application du RGPD.

8. Quelles peuvent être les bases légales des traitements des données à caractère personnel ?

☒ Un contrat

□ Une écoute illégitime d'une conversation

☒ Le consentement

2 Mettre le SI en conformité avec le RGPD, p. 48

1. Visionnez la vidéo, puis présentez les étapes recommandées pour assurer la mise en conformité d'un SI avec le RGPD.

Les étapes recommandées pour assurer la mise en conformité d'un SI avec le RGPD sont les suivantes :

- mesurer le niveau de maturité de la conformité du SI avec le RGPD ;
- mesurer les écarts de conformité des traitements avec le RGPD ;
- étudier comment se mettre en conformité pour réduire les écarts constatés ;
- faire évoluer les processus de l'organisation pour accompagner la mise en conformité ;
- étudier comment protéger au mieux ses données personnelles ;
- faire une analyse de risque (PIA) sur les données.

2. Expliquez en quoi la mise en conformité du SI avec le RGPD est un travail complexe.

La complexité de la mise en conformité du SI avec le RGPD provient du fait qu'il faut réaliser une analyse multiple avec une partie juridique, une partie d'analyse organisationnelle et une partie technique.

3 Repérer les difficultés de la mise en conformité de son SI au RGPD, p. 48

1. Identifiez les articles de la charte répondant aux exigences légales en matière de protection des données à caractère personnel.

Article 2 : il est précisé dans cet article le type de données collectées par le site et leurs destinations. Il est également mentionné comment activer son droit d'accès, de retrait, de modification ou de rectification des données.
Article 3 : il est indiqué le nom de la personne responsable des traitements réalisés par Publigo.
Article 4 : cet article répond au besoin de présenter aux utilisateurs les finalités des données collectées.
Article 6 : il est précisé en quoi les collectes de données reposent sur des situations légales et conformes au RGPD.
Article 7 : les mesures de sécurité des données collectées sont précisées dans cet article.
Article 8 : la durée de conservation des données collectées est indiquée conformément à la demande du RGPD.

2. Analysez les éléments de mise en conformité du SI avec le RGPD et montrez que c'est un travail complexe.

La mise en conformité avec le RGPD repose sur une charte de politique de confidentialité et d'utilisation des données personnelles qui doit couvrir l'ensemble des attentes du texte réglementaire. Vu le nombre d'articles mentionnés à la question précédente, la rédaction de cette charte nécessite une analyse préalable des traitements qui seront réalisés avec les données afin de déterminer le cadre réglementaire de leur collecte. Cette analyse préalable prouve la complexité du travail de mise en conformité du SI avec le RGPD.

4 Vérifier la conformité de la politique de protection des données personnelles, p. 49

1. Vérifiez la conformité du processus de recrutement avec la législation sur la protection des données à caractère personnel (annexe 1).

L'annexe 1 montre que des données personnelles sont collectées (nom, prénom, adresse, téléphone…). Il y a donc une obligation de respect du RGPD.
La protection des données personnelles n'est actuellement pas assurée (un identifiant et un mot de passe uniques pour tous les salariés de l'accueil).
La durée de conservation des données collectées n'est pas en adéquation avec la finalité des traitements réalisés. Une durée indéterminée n'est pas envisageable.

2. Analysez les éléments techniques qui pourraient rendre vulnérable la protection de données personnelles (annexe 2).

Les éléments techniques qui pourraient rendre vulnérable la protection des données personnelles sont les suivants :

- un identifiant et un mot de passe uniques pour les salariés de l'accueil ;
- l'utilisation du protocole FTP qui n'assure pas le cryptage des données transférées ;
- dans le schéma réseau, il apparaît que l'utilisateur peut saisir ses informations directement sur une application mobile. Cette démarche demanderait à auditer la sécurité du code de l'application ainsi que les flux entre la solution mobile du client et le serveur de bases de données ;
- un audit des règles du pare-feu doit également être engagé pour vérifier la pertinence des filtrages ou des détections d'intrusions paramétrés.

5 Organiser une sensibilisation des collaborateurs à la protection des données personnelles, p. 50

1. Retrouvez dans cet article les éléments de sensibilisation des collaborateurs à la protection des données personnelles (annexe).

Voici les éléments de sensibilisation retrouvés dans l'annexe :

- un rappel de la finalité de la collecte des données ;
- une présentation de situations à risques avec des solutions envisageables ;
- un rappel de l'obligation d'alerter en cas de fuite de données ;
- l'utilisation de supports divers comme des vidéos, quiz, mises en situation ;
- la rédaction collaborative d'une charte informatique.

2. Expliquez la phrase soulignée, selon laquelle la sensibilisation des collaborateurs doit s'inscrire sur le long terme.

Une politique de sensibilisation des collaborateurs doit être régulièrement renouvelée afin de prendre en compte les changements des processus métiers de l'organisation et conserver une vigilance en matière de sécurité des données. La politique de sécurité des données de l'organisation doit s'adapter aux changements et les collaborateurs doivent être à l'initiative de ces changements tout au moins en comprendre leurs finalités.

Évaluation 1

Missions

1 Analyser les risques sur les traitements des données à caractère personnel, p. 52

1.1. Repérez les vulnérabilités organisationnelles et technologiques sur la protection des données à caractère personnel.

Vulnérabilités organisationnelles

- Une erreur de saisie peut être réalisée par le responsable de l'agence lors des changements qu'il peut apporter sur les données à caractère personnel.
- Le directeur de l'agence communique parfois ses identifiants de connexion à d'autres salariés ce qui revient à leur donner ses droits de suppressions, d'insertions, de modifications (voir document 2) sur les données contenues dans la base de données.

Vulnérabilités technologiques

- Le protocole de transfert de fichiers vers le serveur de fichiers est réalisé avec le protocole FTP sans cryptage des données (développement à la question 1.2.).
- L'identifiant et le mot de passe utilisé pour accéder au transfert de fichiers sont les mêmes que ceux utilisés pour l'accès à la base de données. Une personne malveillante pourrait accéder à l'un de ses identifiants de connexion et ainsi avoir accès à la fois aux données contenues dans la base mais également aux fichiers stockés sur le serveur de fichiers.

1.2. Précisez en quoi le protocole utilisé pour le transfert de fichier ne permet pas de répondre à l'ensemble des critères de sécurité.

Les critères de sécurité sont : la disponibilité, la confidentialité, l'intégrité et la preuve (voir fiche savoirs technologiques 2).
Le protocole FTP ne permet pas à lui seul d'assurer l'intégrité des données parce qu'il n'assure pas leur cryptage. Une personne malveillante peut écouter les informations communiquées via ce protocole et les lire facilement. On dit que les données sont véhiculées en « clair ».

1.3. Commentez le niveau de risque diagnostiqué pour le traitement des inscriptions.

La cartographie présentée dans le document 4 présente un niveau de **risque inacceptable** pour les traitements des inscriptions.
Le niveau de gravité 4 précise que le risque sur les données traitées lors du processus d'inscriptions des clients peut entraîner des conséquences très importantes pour l'organisation Terre & Mer85.
De plus, le risque sur le traitement des données lors de l'inscription d'un client paraît très vraisemblable (niveau 3), c'est-à-dire qu'il a de fortes chances d'être avéré.

2 Mettre en conformité le traitement des inscriptions des clients avec la législation, p. 52

2.1. Identifiez, parmi les engagements du prestataire ITCloud, ceux qui peuvent aider à la mise en conformité de la protection des données personnelles.

Dans les engagements listés par le prestataire ITCloud (document 5) certains permettent d'aider à la mise en conformité de la protection des données personnelles :

- lorsqu'une zone de stockage est sélectionnée dans l'Union européenne, ITCloud s'engage à ne traiter les données que dans un pays de l'UE et assure que celles-ci ne seront pas traitées aux États-Unis ;
- en cas de violation d'informations, ITCloud s'engage à prévenir ses clients dans les meilleurs délais ;
- une sécurisation des infrastructures de stockage est assurée par ITCloud tout en rappelant que le client reste responsable de la sécurisation de ses applications.

2.2. Rédigez une note dans laquelle vous proposez une liste des solutions techniques et organisationnelles qui permet la mise en conformité de la protection des données à caractère personnel pour le traitement des inscriptions.

Monsieur,

Le traitement des inscriptions des clients par votre organisation révèle plusieurs vulnérabilités d'ordre organisationnelles ou technologiques (voir question 1.1.).

Ainsi, la cartographie des risques sur le traitement des données montre un risque actuellement inacceptable sur les données à caractère personnel (voir question 1.2.).

Une mise en conformité de la protection des données à caractère personnel doit ramener ce niveau de risque à un niveau « acceptable sous contrôle ».

Pour cela il faut réduire le niveau de gravité du risque. Ceci peut être réalisé en proposant de revoir l'organisation de la base de données actuelle en séparant les données à caractère personnel des autres et en y associant des droits d'accès différents et propres à la fonction de chaque utilisateur.

Le niveau de vraisemblance du risque peut être réduit par une gestion plus rigoureuse des mots de passe et un cryptage des données transférées. L'utilisation d'un protocole TLS (*transport layer security*) permettrait d'assurer le cryptage des données pendant leur transport.

Chapitre 3
Préserver l'identité numérique de l'organisation

Missions professionnelles

1 Protéger l'identité numérique de l'organisation, p. 58

1. Repérez, sur le site défiguré, les éléments se rapportant à l'identité numérique de M@Banque.

L'identité numérique est constituée de l'ensemble des contenus diffusés sur Internet permettant d'identifier M@Banque. Trois composantes de l'identité numérique peuvent être distinguées : l'identité déclarative, l'identité agissante et l'identité calculée.
Au regard de cette définition, les éléments se rapportant à l'identité numérique de M@Banque sur le site défiguré sont des éléments de l'**identité déclarative**, à savoir : son nom, son logo et son adresse Web.

2. Identifiez les risques économiques et juridiques encourus par M@Banque suite à la défiguration de son site et à l'accès à des données personnelles de ses clients.

La défiguration du site de M@Banque est la conséquence d'une cyberattaque qui porte atteinte à l'e-réputation de l'organisation sur Internet. Le principal objectif de l'attaquant est apparenté à du dénigrement mais les conséquences sont multiples :

- **au niveau économique :** un ralentissement de l'activité, l'indisponibilité du site Web, la perte de chiffre d'affaires, le départ de clients et la perte de nouveaux clients ;
- **au niveau juridique :** les utilisateurs peuvent se retourner au civil et/ou au pénal en cas de vol des données personnelles.

L'incrimination principale qui peut être retenue ici est celle de l'entrave à un système de traitement automatisé de données (STAD ou système d'information).
Les articles 323-1 à 323-7 du Code pénal disposent :

- le fait d'accéder ou de se maintenir, frauduleusement dans un système de traitement automatisé de données (par exemple en utilisant le mot de passe d'un tiers ou en exploitant sciemment une faille de sécurité) ;
- le fait d'introduire frauduleusement des données dans un système de traitement automatisé de données. Ce texte peut s'appliquer dans le cadre de la défiguration de site. La défiguration désigne la modification non sollicitée de la présentation d'un site web, à la suite d'un piratage du site ;
- le fait d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données d'un système de traitement automatisé de données. La copie frauduleuse de données (souvent improprement qualifiée de « vol » de données) pourra être donc sanctionnée sur ce fondement ;
- le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données ;
- les tentatives de ces infractions sont punies des mêmes peines.

En fonction du cas d'espèce, les peines encourues sont de deux ans à sept ans d'emprisonnement et de 60 000 € à 300 000 € d'amende.

Source : https://www.cybermalveillance.gouv.fr

3. Identifiez la vulnérabilité détectée par la lecture du fichier de journalisation du serveur FTP en indiquant les critères de sécurité défaillants.

Le serveur FTP est bien sécurisé par les protocoles SSL ou TLS qui permet de chiffrer la communication. Toutefois, une faiblesse existe au niveau du mot de passe à 5 caractères. Enfin, l'interface de configuration du serveur FTP permet d'identifier que le paramétrage par défaut permet à n'importe qui de se connecter au serveur.

4. Proposez une solution technique immédiate à cet acte frauduleux, puis recommandez une démarche pour remettre le site en bon état de fonctionnement.

Il est recommandé :

- de désactiver les accès anonymes sur les services FTP en établissant une liste blanche ;
- d'effectuer des sauvegardes régulières des données hébergées ;
- d'utiliser une politique de mots de passe robuste pour les accès aux services.

5. Rédigez une note à l'attention de M^{me} Schmitt pour l'informer des moyens de protections juridiques qui peuvent être mobilisés pour protéger l'identité numérique de M@Banque.

Mme Schmitt,
pour protéger l'identité numérique de M@Banque, il est possible d'agir :

- **en amont,** par la protection des éléments d'identification numérique comme le nom de domaine. La réservation du nom de domaine suit la règle du « premier arrivé, premier servi ». Il est aussi conseillé d'enregistrer son nom de domaine sous la forme d'une marque ;
- **en aval,** par l'établissement d'une preuve de l'acte délictuel pour prouver l'usurpation d'identité. Deux éléments doivent être apportés : un élément matériel et un élément intentionnel. Le constat d'huissier est un moyen de preuve sûr.

2 Déployer les moyens appropriés de preuves électroniques, p. 61

1. Identifiez les éléments permettant de détecter que le courriel contenant un contrat dématérialisé est frauduleux.

À partir des recommandations de la **CNIL** (document 2), il est possible de relever les éléments suivants :

- le caractère peu personnalisé dans la formule de salutation au début du message ;
- le sujet du courriel est vague : l'ouverture d'un compte bancaire ;
- les demandes étranges portant sur l'identifiant et le mot de passe pour accéder aux comptes actuels ;
- le « s » ajouté à « mabanque » dans l'adresse mail de l'expéditeur.

2. Déterminez le délit et les peines encourues par les pirates pour cet acte de malveillance.

Dans le cas présent, l'intention de commettre des actes répréhensibles semble être l'objectif poursuivi. De ce fait, l'usurpation d'identité peut être ici punie de 5 ans d'emprisonnement et de 75 000 euros d'amende.

3. Démontrez que la solution proposée pour les échanges de contrats dématérialisés répond bien aux exigences de la législation.

M@Banque donne deux indications très précises sur la validité d'un contrat dématérialisé :

- l'authentification claire des signataires par l'utilisation d'un logiciel de signature électronique ;
- l'intégrité des documents échangés par l'utilisation du cryptage et la conservation dans un coffre-fort électronique.

Ces deux conditions correspondent aux attentes du législateur par rapport aux conditions de recevabilité de la preuve électronique (article 1316 du Code civil).

4. Présentez les avantages d'une telle solution pour les clients et pour le rétablissement de l'e-réputation de M@Banque.

M@Banque propose un coffre-fort numérique certifié sans intrusion possible.
Pour le client, c'est tout d'abord la possibilité de disposer d'un espace d'échanges et de stockage sécurisé avec son conseiller bancaire. Il pourra retrouver en un seul endroit et depuis n'importe quel terminal mobile l'ensemble de ses informations bancaires. Terminé pour lui le besoin d'archivage papier.
Pour la banque, il est nécessaire de montrer qu'elle se soucie de la sécurité des données de ses clients. La garantie de l'intégrité des documents stockés, l'accès sécurisé et le chiffrement des opérations doivent redonner confiance au client. En effet, les nouvelles fonctionnalités déployées par M@Banque à destination de ses clients montrent les préoccupations de l'organisation à garantir un niveau de service optimum face aux risques des cyberattaques.

Travaux en laboratoire

1 Protéger l'identité numérique de M@Banque, p. 65

1. Complétez le tableau d'organisation de la veille technologique.

Le tableau doit comparer plusieurs sources d'information retrouvées par l'étudiant pouvant l'aider dans sa veille. Les sources d'information choisies par l'étudiant peuvent provenir de différents supports (sites, blog, magazine, livre, vidéo…).
Pour ce corrigé, deux exemples sont proposés.

Objectif de la veille technologique	Comparer des solutions permettant l'audit du site Web de M@Banque					
Sources d'information	Crédibilité de l'auteur	Fiabilité de la source	Objectivité de l'information	Exactitude de l'information	Actualité de l'information	Pertinence de l'information
Blog : blog.hubspot.fr/marketing/outils-seo-analyser-site	1 Erell Le Gall (blogueuse pour la société HubSpot)	1 (Société commerciale HubSpot)	2 (Société commerciale qui propose des logiciels favorisant le référencement de site)	2 (Société commerciale HubSpot)	3 (16/08/2018)	3 (L'article répond au sujet traité.)
Site : https://www.journalducm.com/realiser-audit-site-web/	3 Robert Foban (Auteur de nombreux articles et titulaire d'une licence en Ingénierie Informatique)	3 (Média de référence pour les *community managers*)	3	3	4 (15/07/2019)	3 (L'article mentionne une méthode d'audit de site Web mais pas de solution applicative)

Chaque critère d'évaluation de la qualité et de la pertinence de l'information sera noté de 1 à 4 (1 étant la note signalant que le critère n'est pas du tout respecté).

2. Préparez et paramétrez un dispositif de veille juridique sur les outils d'audits de sécurité de sites Web. Ce dispositif doit comprendre un outil de collecte, de traitement, de curation, de partage de l'information.

Il s'agit ici de préparer et de paramétrer un **dispositif de veille technologique** et non de veille juridique. Ce travail peut prendre appui sur la fiche méthode 2, p. 205.
L'objectif, pour les étudiants, est de comprendre le processus d'une veille technologique (fiche méthode 1) et de maîtriser les outils qu'elle met en place. Plusieurs outils sont présentés dans la fiche méthode 2 mais la liste n'est pas exhaustive.

3. Retrouvez au moins deux autres outils d'audits de sécurité de sites Web à l'aide des résultats de vos recherches.

Voici deux exemples d'outils supplémentaires d'audit de sécurité d'un site web :

- **Dubbed Observatory** (https://observatory.mozilla.org) : outils de vérification des mécanismes de sécurité développés par un ingénieur en sécurité de Mozilla. Il évalue notamment la configuration SSL/TLS (cf. article sur le sujet : https://www.lemondeinformatique.fr/actualites/lire-mozilla-lance-un-outil-gratuit-d-analyse-de-la-securite-des-sites-web-65748.html).
- **Skipfish** (https://code.google.com/archive/p/skipfish/downloads) : scanner Open Source destiné à auditer la sécurité des sites et des applications web. Il a été développé par Google (cf. article sur le sujet : https://www.lemondedupc.fr/article/61/skipfish--un-scanner-de-vulnerabilite-pour-les-sites-web-developpe-par-google).

4. Testez les outils d'audits de sécurité de sites Web en prenant pour cible celui de votre principal concurrent. Complétez le tableau comparatif mis à disposition.

Critères d'analyse	Google Safe-Browsing	UrlVoid	Dubbed Observatory	Skipfish
Protection des cookies			Pas de faille de sécurité	
Content security policy (abrégé CSP) est un mécanisme de sécurité standardisé permettant de restreindre l'origine du contenu (tel qu'un script Javascript, une feuille de style, etc.) dans une page web à certains sites autorisés. Il permet notamment de mieux se prémunir contre des attaques d'injection de code.			Faille mise en avant avec possibilité d'injection de code.	
Utilisation du protocole HTTPS			Pas de faille de sécurité	Pas de faille de sécurité
Spywares*, virus ou *adwares		Seul le site : http://www.websecurityguard.com précise que le site www.n26.com contient des *spywares*, virus ou *adwares*.		
Injection de code SQL ou XML				Pas de faille de sécurité
Site douteux	Aucun contenu suspect détecté	Aucun contenu suspect détecté		

5. Rédiger une note à l'intention de M^{me} Schmitt, la *community manager*, afin de lui fournir les informations lui permettant d'adresser aux clients un courrier présentant clairement la nécessité d'utiliser la solution retenue pour vérifier l'intégrité du site de M@Banque.

La réponse apportée dépend des solutions envisagées et comparées.
La note doit, dans un premier temps, justifier la nécessité de mettre en place un logiciel d'audit de site Web (repérer des failles de sécurité du site de M@Banque afin d'optimiser sa protection) et, dans un second temps, elle doit reprendre des éléments du tableau comparatif afin de valider le choix d'une solution en particulier.

2 Déployer des moyens de preuves sécurisés et conformes à la législation, p. 67

1. Importez les deux machines virtuelles dans votre logiciel de virtualisation (par exemple, VirtualBox) afin d'obtenir l'environnement de test.

💻Importation des machines virtuelles : Chapitre 3-Laboratoire-Delagrave.ova
Les étudiants vérifient les paramétrages réseaux (document 1) et la communication entre les deux machines virtuelles.
Ensuite, ils ajoutent une deuxième carte réseau avec un accès par pont pour disposer d'un accès internet et le testent.

2. Paramétrez les comptes de messagerie client Thunderbird sur les deux machines virtuelles.

- Créer les deux adresses de messagerie (celle de M@Banque et celle du client)

Il vous suffit de créer deux adresses de messagerie sur gmail par exemple :
- mabanque@gmail.com
- clientmabanque@gmail.com

- Créer un compte de messagerie dans Thunderbird pour chaque utilisateur

Les étudiants doivent saisir leurs informations propres à chaque utilisateur :
- VM utilisateur mabanque : création du compte mabanque@gmail.com dans Thunderbird ;
- VM utilisateur clientmabanque : création du compte clientmabanque@gmail.com dans Thunderbird.

- Télécharger le module pour choisir le français comme langue de l'interface : Français Language Pack

Aller sur l'onglet *Add-ons* de Thunderbird et rechercher le pack : Français Language Pack. Installer le pack puis redémarrer Thunderbird.

- Ajouter le module complémentaire Enigmail dans Thunderbird afin d'intégrer le chiffrement PGP dans Thunderbird

Même démarche que pour le pack de langage, il suffit de rechercher et d'installer le module « Enigmail ».

- Dans le module complémentaire « Enigmail », aller dans « Gestion des clés » et modifier les phrases de passe pour les clés de chaque utilisateur.

Aller dans « Enigmail » puis « Gestion des clés » et l'onglet « Générer nouvelle biclé ».
- VM utilisateur mabanque : création d'une nouvelle biclé avec la phrase de passe : mabanque.
- VM utilisateur clientmabanque : création d'une nouvelle biclé avec la phrase de passe : clientmabanque.

3. Testez l'envoi de courriels entre les deux acteurs et vérifiez si le contenu du message est crypté.

Le test doit démontrer que le contenu du message n'est pas crypté.

4. Téléversez les clés publiques sur un serveur de clés dédié afin d'assurer le cryptage du contenu des messages.

Sur chaque machine virtuelle, il faut téléverser les clés publiques puis aller rechercher la clé publique du correspondant afin de pouvoir crypter les contenus des messages.

- **1re étape : téléverser les clés publiques**

Attention de ne pas oublier de confirmer le téléversement en répondant à la vérification par courriel.

- VM utilisateur mabanque : téléversement de la clé publique du compte de mabanque
- VM utilisateur clientmabanque : téléversement de la clé publique du compte clientmabanque

- **2e étape : rechercher les clés publiques**
  - VM utilisateur mabanque : rechercher la clé publique du compte de clientmabanque
  - VM utilisateur clientmabanque : trechercher la clé publique du compte mabanque

En cas de difficulté pour retrouver une clé publique dans le serveur de clé d'Enigmail, les étudiants peuvent envoyer les clés publiques via un mail : Gestion des clés = > Fichier = > Envoyer des clés publiques par courriel.

5. Testez l'envoi de courriels cryptés entre les deux utilisateurs en indiquant les éléments qui permettent de vérifier si l'envoi est bien sécurisé.

Chez l'expéditeur : la passe phrase est demandée pour pouvoir crypter le message (exemple : pour mabanque@gmail.com ce sera mabanque).
Chez le destinataire : la passe phrase du destinataire sera demandée pour décrypter le message reçu (exemple : pour clientmabanque@gmail.com ce sera clientmabanque).
L'empreinte de la clé de l'expéditeur via les algorithmes EDDSA et SHA256 est également visible afin d'apporter la preuve de l'acte.

6. Rédigez un rapport sur les tests réalisés qui démontre que l'utilisation du chiffrement PGP répond à un besoin de renforcement des moyens de preuves sécurisés.

L'ensemble du travail en laboratoire démontre que l'utilisation d'une paire de clés (publique/secrète) permet de renforcer la sécurité en assurant l'intégrité du contenu des messages. Le cryptage par la clé publique rend illisible en « claire » le contenu du message.
L'empreinte de la clé par les algorithmes EDDSA et SHA256 permet d'assurer la preuve de l'identité de l'expéditeur.

Applications

1 QCM, p. 75

1. Sur Internet, l'e-réputation est générée par :

□ les traces numériques officielles.
□ les traces numériques non officielles.
☒ les traces numériques officielles et non officielles.

2. Quels sont les risques pour une organisation en cas de cyberattaque ?

☒ Des risques économiques
☒ Des risques juridiques
☒ Des risques sur son identité numérique

3. L'écrit sur support électronique peut avoir la même force probante que l'écrit sur support papier :

☒ Vrai
□ Faux

4. Quelles sont les conditions de recevabilité de la preuve électronique ?

☒ La personne dont elle émane doit pouvoir être dûment identifiée.
☒ L'information numérique collectée est bien conforme à l'information originale.
□ La preuve doit obligatoirement être certifiée par un organisme d'État.

5. Par qui est délivré un certificat électronique ?

□ L'organisation elle-même
☒ Une autorité de certification de confiance
□ Les clients de l'organisation

6. L'empreinte numérique permet de vérifier :

☒ l'intégrité de la preuve électronique.
□ la confidentialité de la preuve numérique.
□ la disponibilité de la preuve numérique.

7. Un SMS peut être considéré comme une preuve parfaite :

□ Vrai
☒ Faux

8. Le risque économique d'une cyberattaque peut-être :

☒ un ralentissement de la production.
☒ une baisse de la motivation du personnel.
□ une indisponibilité du site Web.
☒ une perte du chiffre d'affaires.

9. Comment l'organisation peut-elle hiérarchiser les risques entre eux ?

☒ Par un calcul du risque acceptable
□ Suivant les compétences du personnel de la DSI
□ En fonction de la date de la cyberattaque.

10. Les risques d'atteintes à l'identité de l'organisation sont :

□ l'arrêt du serveur d'application de l'organisation.
☒ la défiguration du site Web de l'organisation.
☒ l'usurpation de l'identité de l'organisation.
□ une coupure électrique dans la salle des serveurs.

2 Protéger l'identité numérique contre l'empoisonnement du serveur DNS, p. 76

1. Retrouvez la composante de l'identité numérique visée par la cyberattaque de Tradec.

Le nom de domaine ou IDN (*internationalized domain name*, « nom de domaine internationalisé ») est la composante technologique de l'identité numérique de Tradec qui est visée par la cyberattaque.
Plus exactement, avec une localisation du site en Belgique, on a fait une modification du TLD (*top-level domain* ou domaine de premier niveau).

2. Décrivez brièvement chaque étape de la cyberattaque contre Tradec (annexe).

Étape 1 : le pirate envoie une requête vers le serveur DNS de Tradec demandant la résolution du nom d'un site dont la résolution est sous l'autorité du domaine du pirate (dans notre exemple, officiel.com).
Étape 2 : Le serveur DNS de Tradec relaie la requête vers le serveur d'autorité pour la machine demandée qui est le serveur DNS du pirate (domaine : officiel.com).
Étape 3 : Le serveur DNS du pirate envoie ensuite, en plus de la réponse de résolution, des enregistrements complémentaires (mappage entre des noms de sites et des adresses IP fausses). Les enregistrements complémentaires sont mis en cache du service DNS de Tradec.
Étape 4 : Le pirate reçoit la réponse de sa demande de résolution pour la machine qui est bien dans son domaine (officiel.com).
Étape 5 : Un salarié fait une demande de résolution de nom vers un site Web externe.
Étape 6 : Le pirate avait modifié le cache pour la résolution vers ce site. Ainsi la requête est redirigée vers un serveur Web pirate afin de récupérer des identifiants et mots de passe.
Étape 7 : Le serveur Web pirate répond favorablement à la requête du salarié.
Étape 8 : Le salarié a, sur son navigateur, un faux site Web lui demandant son identifiant et mot de passe… Le pirate dispose alors de l'ensemble de ces informations confidentielles.

3 Simuler un empoisonnement du serveur DNS, p. 77

1. Réalisez la maquette de votre environnement de test à l'aide du simulateur Packet Tracer.

💻Fichier Cisco Packet (tracé avant le piratage) : Ch3-Application3-avant-piratage.pkt
💻Fichier Cisco Packet (tracé après le piratage) Ch3-Application3-apres-piratage.pkt

2. Mettez en place l'environnement de tests en respectant le cahier des charges (annexe 2).

L'étudiant doit reprendre les éléments de la maquette présentée dans la question 1 et refaire les tests de connectivité et de résolution DNS.

3. Rédigez le script qui sera transféré depuis le poste du pirate et exécuté sur le serveur DNS afin de modifier l'adresse IP de résolution du site Tradec.

Plusieurs possibilités peuvent être déployées.
Exemple sous linux avec le DNS BOND9 :
Il sera attendu au minimum un script permettant de modifier l'enregistrement de type A dans le fichier de la zone de résolution directe (exemple : /etc/bind/db.tradec.lan) :

- Avant le piratage, la ligne dans la zone de résolution directe :
  www IN A 172.16.1.1
- Après l'utilisation du script : www IN A 172.16.1.2

On peut imaginer une copie du script db.tradec.lan avant la modification puis l'enregistrement de ce même script après la modification.

4. Réalisez les tests d'accès au site tradec.lan depuis le poste du salarié.

Deux tests doivent être proposés : l'un avant le piratage pour vérifier l'accès au site officiel puis l'autre test après le piratage pour constater l'accès au site piraté. Les deux tests doivent être effectués depuis le poste du salarié avec le même URL : www.tradec.lan.

5. Rédigez une synthèse sur les tests réalisés et proposez une solution de sécurisation du service DNS dans le cadre de l'environnement que vous avez mis en place.

La conclusion de cette application doit sensibiliser les étudiants sur les vulnérabilités possibles du service DNS et les orienter sur la recherche de solutions permettant de les limiter.
La première démarche est de mettre régulièrement à jour le service DNS. L'autre démarche est de mettre en place une solution comme DNSSEC qui se base sur des signatures électroniques avec un certificat qui permet d'authentifier les données. L'utilisation du protocole de transport sécurisé TLS peut également limiter l'empoisonnement DNS.

4 Déployer la signature électronique comme moyen de preuve, p. 78

1. Indiquez sous quelles conditions la signature électronique proposée par Fortuneo est une preuve aussi recevable qu'un écrit papier.

Sur le plan juridique, la signature électronique a la même valeur qu'une signature sur version papier. Conformément aux articles 1316-1 et 1366 du Code civil, elle est en effet considérée comme valide tant qu'elle est qualifiée et que :

- l'auteur est clairement identifié ;
- le lien entre l'acte et la personne dont il émane est garanti ;
- l'intégrité de l'écrit signé est assurée ;
- le client a bien manifesté son consentement aux obligations qui découlent de l'acte.

2. Expliquez le rôle de la signature électronique et indiquez comment on peut la vérifier.

La signature électronique est à un document numérique, ce que la signature est à un document papier. Tout comme une signature papier, une signature électronique a pour objectif de démontrer à un tiers que le document a été approuvé par une personne identifiée. Il s'agit d'un mécanisme d'engagement fiable faisant appel à des techniques cryptographiques.
La production d'une signature électronique nécessite l'usage d'un certificat électronique. Ce certificat électronique est assimilable à une carte d'identité numérique permettant d'attester avec certitude de l'identité d'une personne. Il est possible de vérifier une signature électronique si elle est qualifiée, c'est-à-dire si elle est basée sur des certificats délivrés par une autorité de certification qualifiée. Concrètement, il s'agit d'un fichier électronique contenant un certain nombre d'informations personnelles ainsi qu'une clé privée permettant de réaliser des opérations de signature cryptographique.

3. Analysez les avantages de l'utilisation de la signature électronique pour Fortuneo et pour ses clients.

La signature électronique est une innovation gagnant-gagnant pour la banque et les clients en permettant de fluidifier le processus de souscription. Elle permet un gain de temps et d'argent pour l'ensemble des acteurs.
Pour Fortuneo, la signature dématérialisée améliore la gestion en supprimant les risques de perte de documents qui sont toujours disponibles sur l'espace en ligne du client. De plus, la signature électronique présente également un caractère écologique et économique. En effet, elle permet la suppression des photocopies et autres impressions de papiers, d'économiser sur les frais postaux et de réduire les coûts d'archivage.
Pour les clients, elle apporte un certain confort et plus de sécurité. En effet, le contrat est disponible depuis n'importe quel terminal numérique et à tout moment. Tout peut se faire depuis chez soi, en toute sécurité grâce au cryptage des données et avec la garantie d'une prise d'effet immédiate du contrat à sa signature.

4. Identifiez les risques auxquels la banque Fortuneo pourrait être confrontée sans l'utilisation de la signature électronique pour l'acte de souscription en ligne.

En l'absence de signature électronique, si l'acte de souscription en ligne est renvoyé, deux cas peuvent se présenter :

- L'auteur est identifiable et l'intégrité du document est assurée, alors on peut considérer le document comme étant un début de preuve si un écrit « parfait » est exigé par la loi. La validité de l'acte serait laissée à l'appréciation du juge. C'est le cas pour des échanges sur des espaces sécurisés.
- L'auteur et l'intégrité du document ne sont pas assurés, alors l'acte n'est pas valide. C'est le cas des courriels, des SMS et des MMS.

Évaluation 2

Missions

1 Protéger l'identité numérique de l'organisation suite à une attaque par usurpation d'identité, p. 79

1.1. Repérez les éléments dans le coupon de réduction qui permettent de reconnaître une opération d'hameçonnage.

L'hameçonnage (*phishing*) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels en usurpant l'identité d'une entreprise. Les indices pour reconnaître une tentative d'hameçonnage sont :

- les fautes d'orthographe et les erreurs de syntaxe : une faute d'orthographe sur le mot « Cassier » au lieu de « Caissier » et une erreur de syntaxe sur « offre de promotionnelle » ;
- la demande d'informations confidentielles : ici en suivant le lien vers le questionnaire ;
- le caractère urgent et le gain potentiel : pour son anniversaire et le doublement de la réduction ;
- dans le cas spécifique d'un coupon de réduction, de nombreuses mentions légales et obligatoires sont absentes : RCS de l'émetteur, le code coupon et la mention « Traitement ScanCoupon ».

1.2. Identifiez la stratégie utilisée pour obtenir les données personnelles des clients.

La faiblesse psychologique est la principale faille exploitée par l'hameçonnage. En effet, la stratégie utilisée par les pirates s'appuie sur une faille humaine : l'appât du gain avec un prétendu remboursement en faveur des internautes utilisant Facebook.
La mise en confiance est renforcée par la diffusion du message sur le réseau social et le relaye fait par le partage par ou avec des amis de la « bonne affaire ».

1.3. Identifiez les conséquences pour Léandre & Lysandre de tous ces avis négatifs publiés sur les réseaux sociaux suite à cette cyberattaque.

Une attaque de *phishing* réussie peut avoir des conséquences :

- sur l'e-réputation de la marque : avec la méfiance des consommateurs suite à cette mauvaise communication (*bad buzz*) ;
- économique : avec des pertes financières directes dues au ralentissement de l'activité de l'entreprise ou aux coûts générés par des mesures de protection des données ;
- juridique : par les démarches pour la protection de la propriété intellectuelle

2 Déployer les moyens appropriés de preuve électronique, p. 80

2.1. Repérez les éléments dans le message diffusé sur Facebook qui permettraient d'établir une usurpation d'identité.

Deux éléments doivent être apportés pour prouver le délit d'usurpation d'identité : un élément matériel et un élément intentionnel.

- **L'élément matériel :** ici le nom, le logo et la charte graphique de l'enseigne sont largement repris dans le message.
- **L'élément intentionnel :** le faux coupon va générer une perte de confiance des clients et créer un trouble pour l'enseigne qui devra refuser ces coupons.

2.2. Identifiez, dans l'URL de l'adresse de contact et celui du lien fourni, la preuve permettant d'établir cette usurpation d'identité.

Dans l'adresse de contact (document 1), le nom de domaine est : « 2L.leandre.lysandre.com ».
Dans l'adresse officielle (document 6), le nom de domaine est : « 2L.leandre.lysandre.fr ».
La différence entre les 2 sites se situe au niveau du TLD qui a été modifié de « .fr » à « .com ». C'est donc la composante technologique de l'identité numérique de l'organisation qui a été attaquée. En effet, chaque organisation à un IDN unique sur Internet. En profitant d'une faille sur la réservation du nom de domaine, le pirate a pu ainsi créer une copie du site de l'entreprise et récupérer des informations personnelles sur les clients de la marque.

2.3. Rédigez une note à l'intention de M^{me} Chevance sur la conduite à tenir en cas d'usurpation d'identité sur les réseaux sociaux.

M^{me} Chevance,
Les contremesures standards telles que les filtres antispam et protections antimalware ne fonctionnent pas en cas d'usurpation d'identité utilisant le *phishing*. Les logiciels antivirus ne sont pas plus utiles non plus car la plupart des messages de *phishing*, qui sont de mieux en mieux façonnés, ne contiennent souvent aucun *malware*.
La compréhension de la psychologie du *phishing* est un pas en avant vers une meilleure sensibilisation et formation des différents acteurs afin de reconnaître les principes de l'usurpation d'identité s'appuyant sur l'ingénierie sociale.
En cas d'usurpation d'identité sur les réseaux sociaux, il est recommandé de signaler sur la plateforme « PHAROS » (plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements) les sites internet dont le contenu est illicite, mais aussi les messages reçus. Le signalement sera traité par un service de police judiciaire spécialisé : l'office central de lutte contre la criminalité et de la communication (OCLCTIC).
Dans tous les cas, il faut :

- conservez les preuves en constituant un dossier avec les éléments déterminants ;
- déposez plainte auprès des services de police, de gendarmerie ou du procureur de la République ;
- signalez tout message ou site douteux. Il est possible de demander leur suppression directement au responsable du site.

Ces actions sont nécessaires car l'**usurpation d'identité** est un délit (article 226-18 du Code pénal) qui est passible d'une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Enfin, en cas de **Contrefaçon des marques (logos, signes, emblèmes…) utilisées lors de l'hameçonnage**, le délit est passible d'une peine d'emprisonnement de trois ans et de 300 000 euros d'amende (articles L.713-2 et L.713-3 du Code de la propriété intellectuelle).

Chapitre 4
Informer les utilisateurs et mettre en œuvre les défenses appropriées

Missions professionnelles

1 Informer les utilisateurs sur les risques et promouvoir les bons usages à adopter, p. 86

1. Identifiez les situations qui peuvent constituer un risque pour le SI de la MSAP.

Le mot de passe utilisé par le prestataire Enedis est beaucoup trop simple et il est stocké sur un papier à la vue de tout le monde (document 1).
Il n'y a pas de stratégie de sécurité spécifique imposant des contraintes pour la définition des mots de passe. De plus, l'identifiant est similaire au nom de l'organisme partenaire, donc l'usurpation d'authentification est simple (document 2).
La configuration des outils nomades reste à la charge des utilisateurs sans contrôle de l'administrateur système et réseau ni contrainte spécifique. De plus, l'utilisation de supports amovibles de stockage reste une faille de sécurité importante (document 3).
Les partenaires ne semblent pas connaître les bonnes pratiques à adopter face au traitement des courriers électroniques pour éviter les failles de sécurité liées aux spams (document 4).

2. Précisez les bonnes pratiques à adopter par les utilisateurs du télécentre.

Dans un premier temps il faut mettre en place une réelle stratégie de sécurité axée sur l'authentification : définir des mots de passe et identifiants forts selon les critères donnés par l'ANSSI (Fiche savoirs technologiques 4) : un identifiant non nominatif et un mot de passe qui contient au moins 12 caractères alphanumériques, une majuscule et un caractère spécial. La stratégie doit également sensibiliser les utilisateurs quant aux bonnes pratiques liées au stockage des mots de passe et identifiants.
Il faut également réaliser une « campagne » de sensibilisation pour former les utilisateurs d'outils nomades à la configuration du système (mise à jour, correctifs, patches, Packs) et attirer leur attention sur les messages indiquant des failles de sécurité (document 6).

3. Proposez des solutions pour limiter les risques de l'utilisation d'une messagerie.

Les utilisateurs doivent être capables d'identifier un spam (document 4) : adresse de l'expéditeur (free n'utiliserait pas un compte Gmail), erreurs d'orthographe et syntaxe approximative (« afin que vous aidiez à certifier ») et, surtout, ne jamais cliquer sur un lien.
Il faut reconnaître les courriels nommés « coup de fil », demandant de rappeler rapidement, donner des informations personnelles, gagner quelque chose, envoyer des identifiants, faire un transfert d'argent, etc. Le plus souvent, ces messages représentent des attaques par *phishing*.

L'ANSSI recommande de dissocier les adresses personnelles et les adresses professionnelles. Il est même recommandé d'utiliser des adresses « poubelle » lors de l'inscription sur des forums.
Enfin, il est important de traiter les messages de façon correcte : appliquer le marquage comme indésirable pour les messages douteux au lieu de les supprimer simplement.

4. Rédigez la liste des points clés qui devront y figurer

- Stratégie de sécurité liée à la création des identifiants d'authentification : les huit règles de l'ANSSI + la création de *passphrase* + authentification à double facteur (cf. Fiche savoirs technologiques 4, paragraphe IV.1).
- Stratégie de sécurité liée à la configuration des systèmes d'exploitations, des applications et le contrôle des matériels physiques (cf. Fiche savoirs technologiques 4, paragraphe II).
- Stratégie de sécurité liée aux bonnes pratiques quant à l'utilisation des outils Internet (cf. Fiche savoirs technologiques 4, paragraphe IV.2).

2 Identifier les menaces et mettre en œuvre les défenses appropriées, p. 91

1. Précisez la fonction de chacune de ces configurations.

Document 1 : L'outil présenté protège les systèmes contre les *malwares* en contrôlant la signature des applications. Cependant, ici, l'option n'est pas activée ce qui laisse le système sans défense. Les notifications ne sont pas activées non plus, l'utilisateur ne sera donc pas prévenu en cas de présence suspecte.
Document 2 : il n'y a pas d'application configurée sur le poste de travail qui contrôle les entrées et sorties sur le réseau local. Si une tentative d'intrusion est opérée, il n'y a pas de moyen de la détecter et donc de l'empêcher. Il n'y a pas non plus de contrôle des applications, et donc de vérification des signatures de celles-ci. Si une application représente un danger pour le poste de travail, celle-ci pourra donc être exécutée et installée.
Document 3 : les mises à jour automatiques du poste de travail sont désactivées, le poste de travail est vulnérable car les correctifs, patchs et mises à jour ne seront jamais téléchargés ni installés.

2. Identifiez les configurations à modifier pour garantir la sécurité du SI de la MSAP.

Il faut installer une application qui reconnaisse les *malwares* et les empêche d'entrer dans le réseau. Il faut également activer le contrôle permanent des sessions, ainsi que la vérification des nouvelles signatures. Ensuite, il convient d'activer et de configurer une application capable de mettre en œuvre des règles de filtrage en fonction des protocoles, des applications ou des adresses IP, principalement pour contrôler les connexions entrantes. Enfin il faut réactiver les mises à jour automatiques pour que les failles de sécurité soient identifiées et que l'installation des correctifs, etc. soit autorisée.

3. Analysez ces différents outils au regard de configurations étudiées précédemment en justifiant le rôle de chacun d'eux.

L'antivirus permet de vérifier la signature des applications et, donc, d'identifier les applications potentiellement dangereuses pour le système. Pour la gestion de la messagerie professionnelle, il est intéressant d'installer un antispam pour ne pas recevoir de messages indésirables. L'OS Windows permet l'activation des mises à jour automatiques pour connaître les failles de sécurité de l'OS (Windows Update). Enfin l'installation d'un pare-feu permettra de contrôler le trafic entrant et sortant.
L'antivirus, le pare-feu et les mises à jour automatiques sont, a minima, les trois outils indispensables à la sécurité du réseau.

4. Précisez si l'ensemble de ces outils est nécessaire ou si certains peuvent être ignorés.

Certaines applications ne sont pas nécessaires puisqu'elles peuvent être remplacées par des modules. Par exemple, il est inutile d'installer un bloqueur de fenêtres car les navigateurs intègrent cette option. Idem pour les logiciels anti-espions, l'OS Windows intègre cette fonctionnalité.

5. Déterminez l'outil qui répond le mieux à la demande de M. Brillat. Justifiez votre réponse.

L'outil le plus adapté est le serveur proxy qui, grâce à sa *blacklist*, permet une restriction fine. Le redirecteur DNS est efficace mais il demande des connaissances plus poussées car, pour bloquer des sites, il faut connaître leur nom DNS, contrairement au proxy qui opère à partir d'une liste de critères. De plus, il diffuse des publicités.

Travaux en laboratoire informatique

1 Informer les utilisateurs sur les risques et promouvoir les bons usages à adopter, p. 94

1. Présentez le type d'audit que vous allez réaliser auprès de la MSAP.

Le test utilisé sera un « White Hat » car l'ensemble des informations sont données et les tentatives sont réalisées avec l'accord du DSI et avec sa connaissance des tests. Ici, l'objectif est d'identifier une faille de sécurité du SI de la MSAP et d'apporter les configurations nécessaires pour y remédier.

2. Préparez la machine virtuelle Windows de test en reprenant les éléments mentionnés dans le guide de configuration.

Document 2

3. Configurez l'environnement de travail Kali et sauvegardez la partition Windows selon les différentes commandes indiquées.

Document 3

4. Exécutez les différents tests proposés par l'outil John the ripper. Pour cela, appuyez-vous sur les indications détaillées fournies.

La première attaque est une attaque par dictionnaire, c'est-à-dire un fichier texte qui contient un grand nombre de mots de passe déjà définis et qui va les tester tous un à un. L'attaque est réalisée grâce à la première commande du tableau du document 4 et sur le fichier créé lors de la question 3.
La deuxième attaque est une attaque par force brute, c'est-à-dire le test de toutes les combinaisons possibles. Pour réaliser cette attaque avec John the ripper, il faut utiliser la quatrième commande du tableau du document 4, toujours sur le fichier créé dans la question 3.

5. Notez les identifiants trouvés et tirez les conclusions qui en découlent.

Les mots de passe de moins de 8 caractères sont vulnérables même s'ils sont « sophistiqués ».

6. Modifiez le mot de passe du compte Enedis afin de renforcer la sécurité de cette authentification.

Il faut choisir un mot de passe plus long et qui intègre les différentes règles préconisées par l'ANSSI.

7. Proposez, d'après vos observations, au moins un critère qui permette d'améliorer la sécurité des mots de passe.

La longueur semble être le critère le plus important dans la robustesse d'un mot de passe car les attaques par force brute sont capables de casser rapidement un mot de passe court. La modification des lettres comme le « a » par un caractère spécial comme « @ » n'est plus un gage de sécurité car les dictionnaires intègrent ces changements. Enfin il est fort probable qu'un mot de passe qui n'a pas de signification particulière (par exemple des mots quelconques sans rapport mis les uns à la suite des autres) sera plus efficace, c'est pourquoi une passpharse est intéressante.

2 Identifier les menaces et mettre en œuvre les défenses appropriées, p. 97

1. Définissez les objectifs de la veille informationnelle pour répondre à la demande de M. BRILLAT.

Ici, les objectifs sont de connaître les failles de sécurité potentielles sur le système d'exploitation Windows pour assurer l'intégrité du système par l'installation des mises à jour et correctifs. Il faut aussi connaître les nouveaux types d'attaques pour identifier les bonnes pratiques lors du traitement des données et des applications.

2. Identifiez les différentes ressources numériques qui permettront de collecter les informations, en précisant si on peut les qualifier d'informations de qualité. Pour cela, vous dresserez un tableau comparatif des différentes sources, en utilisant les critères suivants : rapidité d'accès, fiabilité, actualité et pertinence.

	Rapidité	Fiabilité	Actualité	Pertinence
Flux RSS – ATOM	Oui (après sélection des sources)	Selon le site de provenance	Oui	Parfois pas assez ciblé, donne trop d'informations
Newsletters	Oui (PUSH)	Idem	Oui	Idem
Forums	Oui / non Cela dépend de la rapidité de réponse des membres	Idem	Pas toujours actuel	Idem Souvent difficile de se retrouver dans les différents files de discussion
Communauté	Oui / non Cela dépend de la rapidité de réponse des membres	Oui souvent spécialisé	Oui si communauté active	Oui souvent ciblé
Réseaux sociaux	Oui / non Si réseau social d'entreprise	Oui / non selon la source (perso ou pro)	Oui	On trouve de tout

3. Comprarez les trois outils de curation présentés dans le document 2, en vous aidant du tableau comparatif du document 3.

Ici, il faut simplement identifier les différents termes et solutions de curations proposées : potion, fils, webmix, etc. Il faut également identifier si ce sont des outils libres ou propriétaires, gratuits ou payants. Si toutes les fonctionnalités sont proposées gratuitement, s'il est nécessaire de créer un compte et s'authentifier. Enfin identifier les différentes sources d'information indexables dans ces agrégateurs.

💻Version du tableau comparatif : CH4_tbl-curation.docx

4. Indiquez de quelle manière vous allez diffuser ces informations. Vous expliquerez les cibles ainsi que les canaux et les supports de communication utilisés.

Cibles	Canaux	Supports
Tous les utilisateurs du SI	Document écrit (charte)	Synthèse des bonnes pratiques
Idem	Intranet	Synthèse des articles
Idem	Newsletters @	Notifications

Applications

1 QCM, p. 103

1. Une charte informatique stipule :

☒ les obligations des signataires.
☒ les sanctions applicables.
□ les modalités de diffusion de celle-ci.

2. Une charte informatique doit obligatoirement être affichée dans les locaux de l'entreprise.

□ Vrai
☒ Faux

3. La charte informatique s'applique :

□ aux salariés de l'entreprise uniquement.
□ aux seuls utilisateurs du système d'information.
☒ à l'ensemble du personnel, quel que soit son statut hiérarchique.

4. La charte informatique est opposable au salarié :

☒ par annexion au règlement intérieur.
☒ par annexion au contrat de travail.
□ quelle que soit la date d'entrée en vigueur.

5. L'organisation à l'initiative de la charte peut imposer un droit de contrôle sur :

☒ la journalisation des accès et des modifications de fichiers.
☒ les connexions à Internet.
☒ les appels téléphoniques.
☒ la messagerie électronique.

6. La sécurité des postes de travail comprend la configuration :

☒ des systèmes d'exploitation.
☒ des applications.
☒ des matériels physiques.

7. La sécurité des postes de travail ne concerne pas l'accès aux données.

□ Vrai
☒ Faux

8. Un antivirus permet :

□ de filtrer les connexions entrantes dans un réseau local.
□ de filtrer les connexions sortantes d'un réseau local.
☒ d'identifier les signatures des *malwares*.
□ de relayer les demandes de connexions vers les serveurs web.

9. Un pare-feu permet :

☒ de filtrer les connexions entrantes dans un réseau local.
☒ de filtrer les connexions sortantes d'un réseau local.
□ d'identifier les signatures des *malwares*.
□ de relayer les demandes de connexions vers les serveurs Web.

10. Un serveur proxy permet de restreindre l'affichage de sites Internet.

☒ Vrai
□ Faux

2 Analysez un outil de protection numérique, p. 104

1. En vous appuyant sur les informations fournies en annexe, recommandez à M. Archi un outil à configurer au sein de son réseau local pour filtrer les connexions Internet.

Il faut utiliser un serveur proxy (patron de conception) qui permet de surveiller les échanges entre des hôtes et des serveurs (ou autres hôtes) et autoriser ou non les connexions.

2. Expliquez de quelle manière cet outil autorise ou non la demande de connexion à un site spécifique.

Il permet, par l'intermédiaire d'une *blacklist*, de rendre impossible la connexion à des sites selon des mots-clés, ou des URL, par exemple, la liste noire d'URL proposée par l'université de Toulouse 1 capitole.

3. Montrez comment l'outil que vous avez proposé peut prendre en charge ces pratiques.

Il permet de mettre en place des règles sur des URL, des adresses IP et aussi sur des protocoles (FTP par exemple qui est le protocole utilisé pour les téléchargements).

4. Précisez s'il permet de se protéger contre les intrusions des *malwares*.

Son rôle n'est pas de vérifier les signatures des applications, cependant les pare-feu logiciels permettent le plus souvent d'intégrer des services supplémentaires comme la détection de *malwares*. Mais cela est moins souple, il est préférable d'installer un outil dédié.

3 Développer une configuration système, p. 105

1. Indiquez comment M. Archi peut intervenir sur les postes de travail pour contrôler l'utilisation des supports USB.

Il peut intervenir sur le BIOS pour empêcher l'exécution automatique des supports amovibles, des ports et lecteurs. Il peut également désactiver le *boot* sur un support amovible.

2. Expliquez quelle précaution supplémentaire il doit prendre pour être certain que la configuration réalisée précédemment soit pérenne.

Il faut intégrer un mot de passe au BIOS.

3. Indiquez quelle application native sous Windows permet d'avoir une version récente du système d'exploitation.

Les mises à jour automatiques (sous Windows on parle de Windows Update).

4. Démontrez que celle-ci peut également agir sur les failles de sécurité.

Les mises à jour automatiques permettent d'installer les correctifs et patchs pour empêcher les vulnérabilités et palier les failles de sécurité identifiées.

5. Précisez quel outil supplémentaire peut être installé sur un poste de travail pour garantir sa sécurité.

Un antivirus permet de définir les signatures des *malwares*. Les dernières versions de Windows permettent également la mise en œuvre d'une protection contre les *ransomware*, le contrôle des applications et du navigateur…

4 Promouvoir les bonnes pratiques, p. 105

1. En vous appuyant sur les informations données par l'ANSSI, indiquez les spécifications qui doivent être mentionnées dans le guide au sujet de la création des mots de passe utilisés par les étudiants pour leurs connexions au réseau local.

Utiliser les règles du guide de l'ANSSI (cf. Fiche savoirs technologiques 4, paragraphe IV) : R1-2-3 + 12 caractères minimum avec la création d'une *passphrase*.

2. Précisez les recommandations à suivre pour la gestion de ces mots de passe durant les deux années du BTS.

Se référer là encore aux règles de l'ANSSI : R5-6-7-8, possibilité aussi d'avoir un gestionnaire ou coffre-fort de mots de passe comme Keepass.

3. Expliquez les deux méthodes utilisées pour définir un mot de passe par *passphrase* (passe de phrase ou phrase secrète).

La méthode phonétique et la méthode des premières lettres.

4. Indiquez quelles manipulations ne sont pas souhaitables, et expliquez pourquoi.

Il ne faut pas permettre l'enregistrement des mots de passe et autres éléments d'authentification car il serait très simple ensuite de pirater les différents comptes principalement l'adresse mail qui est utilisée pour la plupart des autres comptes, achats, etc. De plus, il est intéressant de désactiver la saisie automatique des caractères dans les champs texte pour éviter de donner une indication sur les éléments d'authentification.

5. Expliquez le rôle des différentes stratégies de sécurité locales présentées en annexe.

- Conserver l'historique des mots de passe permet de ne pas réutiliser un même mot de passe.
- La durée de vie maximale du mot de passe impose de changer régulièrement de mot de passe et augmente ainsi la sécurité.
- La durée de vie minimale du mot de passe : le mot de passe ne pourra pas être modifié selon la durée indiquée, empêchant ainsi le changement de mot de passe par l'utilisateur ou un tiers qui aurait de mauvaises intentions.
- Enregistrer les mots de passe en utilisant un chiffrement pour les stocker façon sécurisée car ceux-ci ne sont pas lisibles.
- Exigence du mot de passe : nombre de caractères et type de caractères, indiqué dans le détail de la stratégie.
- Longueur minimale du mot de passe : on indique le nombre de caractères requis.

6. Appliquez ces stratégies sur le compte donné par M. Onnier en définissant un mot de passe.

Dans le *prompt* (commande cmd dans la zone de recherche de la barre des tâches) ou dans la fenêtre de recherche de la barre des tâches, saisir : « secpol.msc » (on peut également saisir dans la zone de recherche de la barre des tâches : « Stratégie de sécurité locale »), puis choisir « stratégies de comptes » puis « stratégie de mot de passe ». L'onglet « expliquer » donne des indications pour la configuration de la stratégie.

5 Gérer les mots de passe, p. 106

1. Consultez le tutoriel sur l'utilisation de Keepass.

2. Installez l'outil KeyPass sur une machine virtuelle (voir travaux en laboratoire 1, p. 94).

Il faut avant tout créer la base de données Keepass qui contiendra tous les éléments d'authentification enregistrés (accès à des applications, des formulaires d'authentification en ligne, etc.). Il faut ensuite choisir le mot de passe principal (celui qui permettra d'ouvrir l'application Keepass) qui est appelé sous Keepass = clé principale. Celui-ci doit être robuste. On peut choisir la génération de ce mot de passe par l'application mais il est préférable de constituer son propre mot de passe pour que celui-ci puisse être retenu plus simplement.

3. Testez les fonctionnalités de l'outil.

Les fonctionnalités importantes sont la possibilité de chiffrer les mots de passe et identifiants mais aussi de conserver en mémoire (presse papier) le mot de passe que pendant 12 secondes, ensuite celui-ci est automatiquement supprimé du presse-papiers ce qui évite qu'on puisse le récupérer ultérieurement.
Keepass renseigne les identifiants pour les applications, les sites internet (URL) et pour les entrées des fichiers (base de données). Le glisser/déposer est possible ou le renseignement automatique. Il permet de créer des sous-rubriques de classement.

4. Dressez un tableau présentant les avantages et inconvénients de celui-ci.

Avantages	Inconvénients
- Conserver l'ensemble des mots de passe de façon chiffrée donc sécurisée. - Ne pas avoir besoin de se souvenir de l'ensemble des mots de passe. - Licence GPL avec une communauté très active qui propose de nombreux *plugins*.	- Si le mot de passe d'ouverture de l'application est trouvé tous les mots de passe seront accessibles. - Si la BDD utilisée par l'application (nom.kdb ou. kbdx) est supprimée tous les mots de passe sont perdus. - Les *plugins* ne sont pas tous testés par KeePass et peuvent donc représenter une faille de sécurité.

Chapitre 5
Sécuriser l'accès aux ressources et vérifier l'efficacité

Missions professionnelles

1 Gérer les accès et les privilèges appropriés, p. 108

1. Identifiez les configurations qui présentent des risques pour la sécurité des données.

Document 1 : les recommandations données par l'ANSSI préconisent de ne pas activer le compte administrateur par défaut avec l'identifiant « Administrateur » car c'est le premier compte qui est piraté et il possède l'ensemble des privilèges. Il est donc nécessaire de créer un compte administrateur qui porte un identifiant différent.
Document 2 : ici deux problèmes : d'abord, chaque compte des partenaires appartient au même groupe. Si une stratégie est réalisée pour le groupe ou encore un partage pour ce groupe, tous les comptes auront accès aux mêmes ressources (notion de groupe et héritage des privilèges aux membres du groupe). Ensuite, on s'aperçoit que le groupe « partenaires » (et donc tous les comptes) possède des droits administrateur qui délivrent alors les habilitations nécessaires pour réaliser l'ensemble des actions.

2. À partir des différentes informations que vous avez relevées, rédigez une synthèse des bonnes pratiques à adopter.

On retrouve les mêmes erreurs commises lors de la création des comptes, à savoir la notion d'héritage.
Documents 3 : donner accès à l'active directory par des utilisateurs autres que l'administrateur représente déjà un point de vulnérabilité. Ensuite, il ne faut pas créer un partage « global » ou « parent » : chaque partenaire devrait avoir un dossier de partage à son nom. Ici, ils possèdent bien ce dossier mais le partage est réalisé sur le dossier parent ce qui signifie que l'ensemble des comptes ont accès à l'ensemble des données présentes dans les différents sous-dossiers. Il serait donc préférable que les partages soient réalisés directement sur chaque dossier dans le dossier « partageTelecentre » mais que celui-ci ne soit pas en partage.
Document 4 : on voit bien que l'ensemble des utilisateurs ont accès au partage, et donc aux données, mais également le groupe « Tout le monde », donc tous les utilisateurs du SI. De plus, ce groupe est en contrôle total, les données peuvent être supprimées. Enfin, avec la deuxième fenêtre, on s'aperçoit que le groupe « Utilisateurs » est aussi autorisé (ACL) à agir sur les données. Il faut forcément, dès que l'on crée un partage, supprimer le groupe « Tout le monde » et le groupe « Utilisateurs » pour ne pas rendre les données accessibles par tous les utilisateurs du SI.

3. Indiquez quel autre problème de sécurité pourrait être provoqué par les privilèges accordés aux utilisateurs.

On voit que le groupe « partenaires » possède également les accréditations sur le dossier « PartageTelecentre » ce qui implique que, même si le groupe utilisateur n'était pas autorisé, l'ensemble des utilisateurs partenaires pourraient avoir accès aux données de chacun. L'ensemble des ACL sont données (modification, lecture, etc.).

4. Précisez les préconisations à adopter quant à la segmentation du SI de la MSAP.

Les différents postes de travail utilisés par les partenaires sont connectés sur le même commutateur. Ils appartiennent donc tous au même domaine de diffusion. Cela pose un problème de sécurité car ils peuvent tous communiquer sans restriction.
Afin d'améliorer la sécurité du LAN, il convient de segmenter le réseau en créant un VLAN pour chaque utilisateur (segmentation logique). Appartenant à un réseau IP différent, ils devront obligatoirement passer par le routeur (passerelle) pour s'échanger des informations. Or, on pourra créer des règles de filtrage ou ACL sur ce routeur.
De plus, même s'ils appartenaient au même sous-réseau IP, le fait qu'ils appartiennent à des VLAN différents, permet de réguler les domaines de diffusion.
Il faudra veiller à ce que chaque port reliant un matériel à un autre soit en 802.1q (trunk) pour que l'ensemble des trames taguées puissent circuler.

2 Vérifier l'efficacité de la protection, p. 111

1. Effectuez un diagnostic de l'efficacité des modifications apportées pour les habilitations et les autorisations.

Document 1 : les utilisateurs qui se connectent ont la possibilité de créer un lecteur réseau sur le serveur de fichiers, c'est-à-dire un accès au dossier de partage qui porte leur nom. Ici, on s'aperçoit que seul l'utilisateur (ouverture de session) qui porte le même nom que le dossier peut créer le lecteur réseau (autorisation d'accéder au chemin réseau du dossier). Les partages ont donc été modifiés : le dossier PartageTelecentre n'est plus partagé (sinon chacun aurait pu créer un lecteur réseau sur chaque sous-dossier).
Document 2 : lors de la tentative d'installation d'une application, on doit s'authentifier en tant qu'administrateur. Donc les comptes utilisateurs n'appartiennent plus au groupe administrateur et n'ont plus les privilèges nécessaires pour l'installation d'applications.

2. Indiquez quelle autre solution serait souhaitable pour améliorer la sécurité du SI.

Les documents 3 et 4 : il s'agit de l'observateur d'évènements Windows, un outil d'administration qui enregistre toutes les activités du système d'exploitation et de ses applications dans des *logs* ou journaux. Ces journaux se présentent sous la forme de fichiers textes classiques reprenant de façon chronologique l'ensemble des évènements qui ont affecté le système (ex. : traçabilité des plantages). Ils correspondent à des codes erreurs appelés *Event ID* et indiquent également l'utilisateur connecté et l'heure de connexion. Le suivi des logs sur les postes de travail est bien activé ce qui permet d'ajouter un niveau de sécurité. Cependant, le document 4 indique qu'il n'y a aucun abonnement configuré. Pourtant, cela permettrait de centraliser le suivi des logs des différents postes. Le poste administrateur devrait représenter le collecteur de journaux et ainsi s'abonner à l'ensemble des postes de travail pour un suivi et une gestion centralisés.

3. Indiquez si la nouvelle infrastructure physique et logique permet d'atteindre les objectifs fixés. Justifiez votre réponse.

Oui la nouvelle infrastructure permet d'atteindre les objectifs car, dans le document 1 (commande « sh vlan » sur le commutateur), les VLANS ont bien été créés et les ports sur lesquels sont connectés les postes de travail sont bien affectés à un VLAN (commande « access »). Les domaines de diffusion sont donc restreints et les utilisateurs doivent passer par le routeur, la passerelle, (sur lequel les interfaces virtuelles ont été créées pour gérer chaque VLAN) pour communiquer entre eux, même s'ils sont connectés sur le même commutateur.
Le document 6 : les différents postes appartenants aux différents VLAN ne peuvent pas communiquer entre eux : le *ping* du réseau 192.168.10.0 /24 vers le réseau 192.168.20.0 /24 est refusé (*acces_list* →*deny ip any any*). Ce n'est pas réellement la réponse du *ping* dans le *prompt* qui permet de voir que c'est une ACL qui a interdit la communication, mais l'analyse de la PDU qui montre la fonction de l'*acces list* nommée : ctsrv. Par contre, le deuxième *ping* vers le serveur de fichier (réseau 192.168.100.0 /24) a été autorisé.
Le document 7 : la commande *tracert* (qui permet d'afficher la route suivie par un paquet pour atteindre sa destination) montre que les hôtes doivent bien passer par le routeur ou leur passerelle (192.168.10.54) pour communiquer, que ce soit pour communiquer avec un autre hôte ou avec le serveur de fichiers : la deuxième adresse IP présentée dans le résultat de la commande indique l'hôte de destination.

Travaux en laboratoire informatique

1 Gérer les accès et les privilèges appropriés, p. 115

1. Préparez la machine virtuelle de tests (second serveur de fichiers) d'après les consignes.

L'objectif du document 1 est de faire réfléchir sur la faisabilité des consignes indiquées, notamment sur le fait que le rôle serveur de fichiers est installé par défaut sur les OS Windows 202 R2.
De plus, la stratégie de sécurité liée au mot de passe n'autorise pas l'utilisation du même mot de passe pour chaque compte. Il faut donc prendre l'initiative de modifier le mot de passe (ou désactiver la stratégie de sécurité « stockage des mots de passe », mais cela n'est pas conseillé).

2. Créez les différents partages en relevant les chemins d'accès qui servent à définir un lecteur réseau pour chaque compte.

Pour cela, il faut créer, dans le dossier « Partage », les sous-dossiers « ENEDIS », « MSA », « CLIC » et « TRESOR ». Ensuite, sur chaque dossier, dans l'onglet « partage », il faut créer le chemin de partage en définissant les autorisations de connexion (uniquement l'utilisateur qui porte le même nom que le dossier partagé).

3. Définissez les autorisations et les ACL (liste de contrôle d'accès) sur les partages en vous appuyant sur les recommandations données.

Il est important de supprimer tous les groupes et utilisateurs qui ne portent pas le même nom que le dossier partagé, afin de donner accès à ce partage uniquement à l'utilisateur concerné.

4. Réalisez les tests.

Message d'erreur qui sera affiché pendant le test : « Windows ne peut accéder à \\chemin_de_partage. » Cela montre que seul l'utilisateur authentifié avec le même nom que le partage est autorisé à accéder aux ressources numériques.

2 Vérifier l'efficacité de la protection, p. 117

💻Fichier Packet Tracer (version prof) : CHP5-Labo2-Prof.pkt

1. Préparez l'environnement de travail d'après les informations fournies.

Il faut relier les différents postes de travail à leurs différents ports sur le commutateur CommutateurTEL selon les indications données : exemple poste ENEDIS sur le port 2.
Pour cela, il ne faut pas utiliser l'outil de sélection des supports réseaux « éclair jaune », sinon le choix du port est réalisé automatiquement sans laisser le choix du numéro. Il est également nécessaire de vérifier que chaque hôte dispose bien d'une adresse IP dans le bon réseau.

2. Configurez le commutateurTEL pour intégrer les VLAN.

Utilisation des commandes suivantes pour chaque VLAN, donc 4 fois en changeant à chaque fois le numéro, le nom du VLAN et ensuite le port :

```
CommutateurTEL #conf t
CommutateurTEL (config)#vlan 10                          numéros du vlan
CommutateurTEL (config-vlan)#name ENEDIS                 //nom du vlan
CommutateurTEL (config)# int fat 0/2                     //port affecté au VLAN
CommutateurTEL (config-if)#switchport mode acces         //on passe en mode access
CommutateurTEL (config-if)#switchport access vlan 10     //sur le VLAN de numéro 10
```

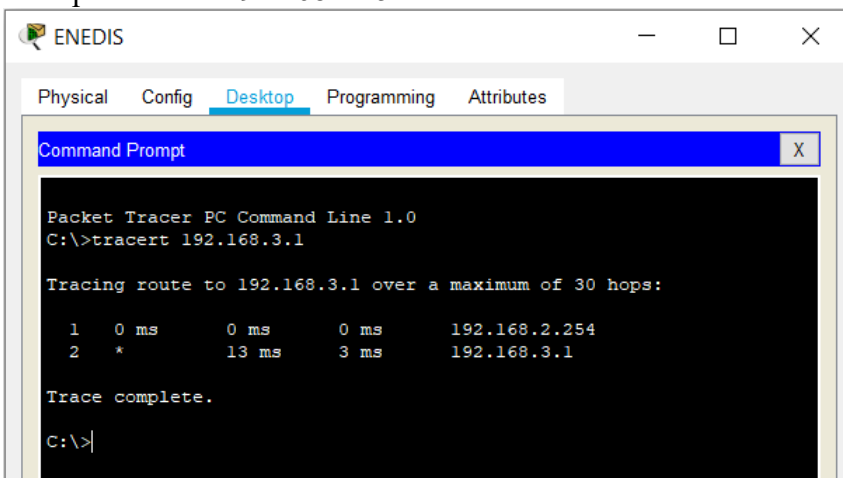
3. Modifiez la configuration sur le routeur principal pour qu'il relie l'ensemble des VLAN.

On doit intervenir sur l'interface GigabitEthernet 0/1. Dans un premier temps, il faut vérifier que cette interface ne possède pas d'adresse IP pour que les commandes qui suivent fonctionnent.
Puis il faut créer autant d'interfaces virtuelles que de VLAN (donc 4 dans ce cas).
Exemple pour le VLAN 10 de nom ENEDIS :

```
RouteurPrincipal #conf t
RouteurPrincipal (config)#int gigabitEthernet 0/1.2          //2 comme sous-interface
RouteurPrincipal (config-subif)#encapsulation dot1Q 2        //2 représente le numéro de VLAN
RouteurPrincipal (config-subif)#ip address 192.168.2.1 255.255.255.0 // réseau logique VLAN 2
RouteurPrincipal (config-subif)#no sh          //elle reste en UP
```

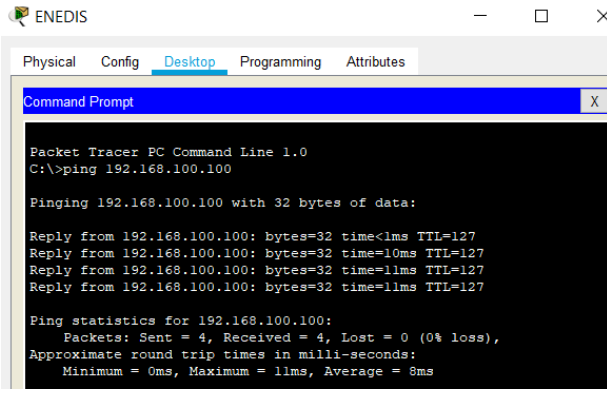
4. Réalisez les tests pour vérifier le bon fonctionnement de l'infrastructure.

Pour le premier test on utilise la commande *tracert*.
Pour la deuxième commande on utilise le *ping*.
Poste ENEDIS (192.168.2.1) contacte le poste MSA (192.168.3.1). Pour l'atteindre, il doit passer par sa passerelle : 192.168.2.254

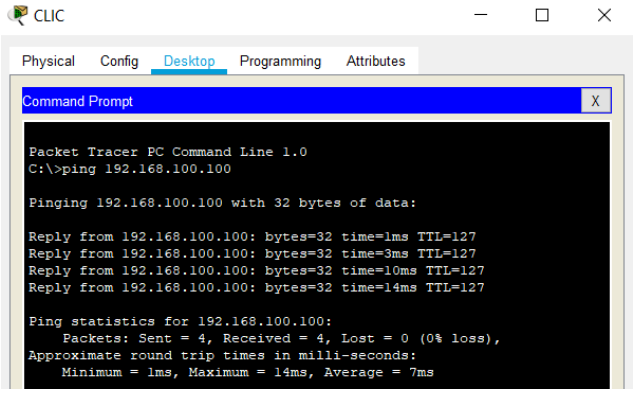


Accès des différents postes clients au serveur de fichiers :

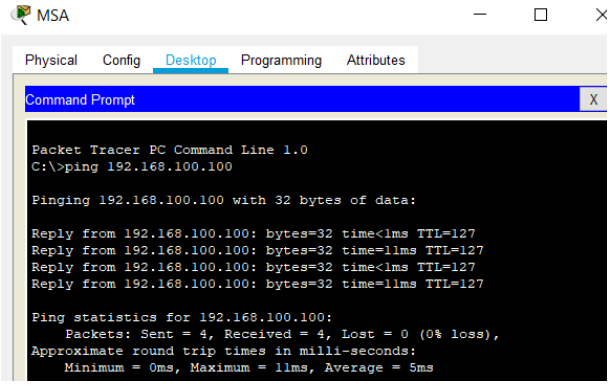
- Poste ENEDIS



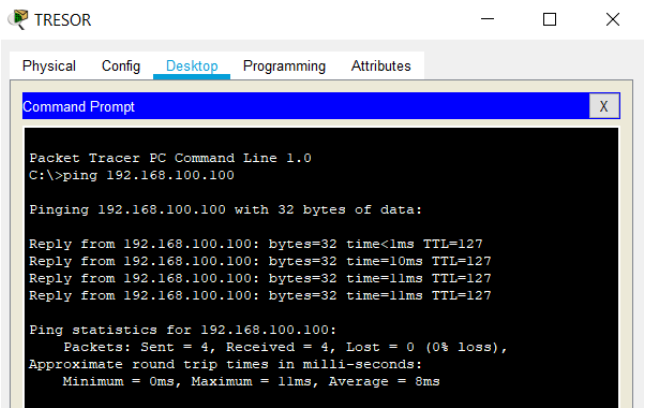
- Poste CLIC



- Poste MSA



- Poste TRESOR



Applications

1 QCM, p. 127

1. Si une organisation fait l'objet d'une violation des données, elle doit obligatoirement la notifier :

☒ auprès de la CNIL.
□ auprès du RGPD.
□ auprès des personnes concernées (propriétaires des données).

2. Si une organisation fait l'objet d'une violation des données, celle-ci doit obligatoirement documenter les violations en interne.

☒ Vrai
□ Faux

3. Le RGPD impose pour toute organisation une obligation de :

☒ mettre en œuvre les mesures techniques pour garantir la sécurité des données.
☒ mettre en œuvre les mesures organisationnelles pour garantir la sécurité des données.
□ mettre en œuvre les mesures comptables et fiscales pour garantir la sécurité des données.

4. L'obligation de notification est inscrite dans le RGPD dans :

□ l'article 32.
☒ l'article 33.
☒ l'article 34.

5. Les responsables de traitement des données doivent réaliser cette notification sous :

□ 24 heures.
□ 48 heures.
☒ 72 heures.

6. La CNIL permet de réaliser cette notification.

☒ Vrai
□ Faux

7. Le cahier des incidents doit comprendre :

☒ la nature de la violation.
☒ les catégories des personnes concernées.
☒ le nombre de personnes concernées.
□ le montant des coûts engendré.

8. En cas de non-respect des obligations, les autorités de contrôle ont la possibilité de sanctionner tout responsable de traitement :

☒ par le biais d'amendes.
☒ par le biais d'un emprisonnement.

9. L'authentification concerne :

☒ l'attribution des éléments d'identification (login et mot de passe).
□ la définition des privilèges pour chaque compte.
□ les autorisations sur les partages.
□ les droits d'accès sur les données.

10. Un commutateur permet de segmenter un réseau local :

☒ de façon physique.
☒ de façon logique.

11. Le cahier des incidents et le registre des traitements désignent le même document.

□ Vrai
☒ Faux

2 Gérer les accès et les privilèges, p. 128

1. Indiquez à M. Rens les bonnes pratiques à adopter en termes d'authentification et d'accréditation (annexe 1 et 2).

Authentification : imposer des contraintes concernant le mot de passe et ne pas permettre d'utiliser un mot de passe similaire au login. Ici, lors de la première connexion, le mot de passe peut être le même que le login car c'est l'administrateur qui crée les éléments de connexion, mais il doit veiller à ce qu'à la première connexion les utilisateurs le modifient obligatoirement (case cochée dans le profil du compte). De plus, les comptes utilisateurs ne doivent pas appartenir au groupe Administrateur
Accréditation : les partages sur le serveur de fichiers doivent être isolés et nommés ; et non tous dans le même dossier de partage.

2. M. Rens est l'administrateur des machines. Expliquez-lui quelles précautions il doit prendre concernant le compte administrateur.

Le compte administrateur par défaut doit être désactivé et le nouveau compte administrateur doit porter un nom différent de RENS. M. Rens doit également veiller à mettre un mot de passe fort. Il ne devra utiliser ce compte que pour des tâches d'administration. Pour les tâches de formation, il peut créer un compte avec son nom mais sans les privilèges d'administration car il sera amené à manipuler des fichiers et à se rendre sur internet.

3. Indiquez quels privilèges il doit accorder à chaque utilisateur (annexe 3).

Il ne doit pas garder le groupe « tout le monde » car chaque utilisateur aura accès aux données des autres. Il doit donc créer un partage différent pour chacun. Concernant les ACL, il doit supprimer le compte « tout le monde » et n'autoriser que les comptes identifiés avec l'ensemble des autorisations car ils seront propriétaires de leurs données.

4. Indiquez ces obligations en précisant pour chacune en quoi elle consiste (annexe 4).

M. Rens doit suivre les recommandations du RGPD. Pour cela, il doit documenter les violations des données personnelles et notifier celles-ci auprès de la CNIL. Il a obligation de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Enfin, il doit mettre en œuvre un cahier des incidents.

3 Sécuriser les communications, p. 130

1. Indiquez à M. Rens de quelle solution il dispose pour segmenter le réseau.

M. Rens peut réaliser une segmentation logique, c'est-à-dire en agissant sur les sous-réseaux IP et en intégrant des VLAN au niveau du commutateur. Il doit créer des VLAN différents pour chaque service et pour la salle Accueil. Il peut, dans un premier temps, isoler tout ce qui concerne l'organisation et, dans un second temps, le VLAN de la salle Accueil. Pour cela, il doit créer des sous-réseaux IP différents et intégrer des interfaces virtuelles sur le routeur afin que les VLAN puissent communiquer ou non selon des ACL spécifiques à chacun.
La salle Accueil ne sera donc plus dans le réseau 1.0 /24

2. Rédigez une procédure pour répertorier les différentes étapes de réalisation de cette segmentation.

- Définir les sous-réseaux IP.
- Commutateur :
  - Créer les différents VLAN dans le fichier vlan.dat (numéro et nom).
  - Affecter les ports en access pour chaque VLAN.
  - Affecter un port en 802.1q (*trunk* entre le commutateur et le routeur).

3. À l'aide d'un logiciel de simulation réseau (Packet Tracer, par exemple), reproduisez l'infrastructure de l'association en appliquant les modifications nécessaires sur le commutateur.

4. Expliquez les conséquences de la segmentation logique du commutateur sur le routeur box (interface physique côté LAN).

- Routeur : créer les différentes interfaces virtuelles sur l'interface physique reliée au commutateur selon le nombre de VLAN.
- Ajouter les ACL pour empêcher que le réseau de la salle Accueil puisse communiquer avec le réseau administratif.

Évaluation 3

Missions

1 Identifier les failles de sécurité liées à la gestion du parc informatique de la salle de formation, p. 132

1.1 Repérez les failles de sécurité liées à la configuration système des postes de travail et au processus d'authentification des utilisateurs.

Les différentes applications qui permettent de sécuriser les postes de travail (antivirus et pare-feu) sont bien installées mais elles sont mal configurées : le pare-feu est désactivé, il n'y a donc pas de contrôle du trafic entrant et sortant.
Le contrôle des applications et du navigateur (inhérent à l'utilisation du pare-feu Windows) est également désactivé ce qui ne permet pas de :

- rechercher les applications et les fichiers non reconnus ;
- contrer les sites et les téléchargements malveillants ;
- d'utiliser « Exploit protection » qui protège contre les attaques de sécurité système.

L'authentification : il n'y a pas de contraintes spécifiques liées à la création des mots de passe. On ne demande pas aux différents utilisateurs de suivre des recommandations (longueur du mot de passe, complexité, etc.). De plus l'enquête montre que, pour la plupart des utilisateurs, les mots de passe choisis sont trop simples et semblent correspondre aux différents mots de passe présents dans les dictionnaires d'attaques.

1.2 Précisez en quoi la procédure d'attribution des autorisations et privilèges sur les dossiers de stockage des données ne permet pas de garantir la sécurité des données de chaque utilisateur.

Il y a bien un sous-dossier spécifique pour chaque utilisateur qui est créé pour le stockage des données. Cependant, ces sous-dossiers sont créés à la racine du dossier PartagesParticipant qui est rendu accessible pour l'ensemble des utilisateurs (tout le monde) sans restriction particulière et en contrôle total (modification, suppression).
De plus, les accréditations gardent le groupe « Utilisateurs authentifiés » et « Utilisateurs » aussi avec un contrôle total. Donc tous les utilisateurs peuvent accéder à l'ensemble des partages avec l'ensemble des privilèges.

2 Mettre en œuvre des configurations et outils pour garantir la sécurité du SI du Greta, p. 132

2.1 Indiquez quelles premières modifications vous pouvez apporter pour corriger les failles de sécurité identifiées précédemment.

Bien entendu, dans un premier temps, il faut réactiver le pare-feu et ainsi garantir une meilleure sécurité des connexions Internet.
Dans un second temps, il convient d'imposer des contraintes lors de la création des mots de passe. Pour cela, le plus simple (même si une sensibilisation avant chaque action de formation semble adéquate) est d'activer les stratégies locales de sécurités liées à la stratégie de mot de passe et ainsi agir sur les différentes options. Toutes les options ne sont pas indispensables (le stockage ne semble pas opportun car la session dure un temps limitée ; idem pour les durées maximale et minimale). Par contre, il est indispensable de contraindre le choix du mot de passe : « le mot de passe doit respecter des exigences de complexité » et « longueur minimale du mot de passe ». L'option chiffrement est également intéressante.
Enfin, il faut créer un partage pour chaque utilisateur sur leur dossier spécifique (en supprimant le partage sur le dossier racine : « PartagesParticipant ») et supprimer les groupes « Tout le monde » et « Utilisateurs » au niveau des autorisations et ACL.

2.2 Détaillez une segmentation possible pour sécuriser davantage les échanges dans le réseau local du Greta.

Il faut réglementer la communication de la salle de formation avec le LAN : on doit garder la possibilité de communiquer avec le serveur DHCP pour recevoir la configuration IP du *pool* Formation. On doit également garder la possibilité de communiquer avec le serveur web et Internet. Il faut donc :
Commutateurs 1 à 4 : créer le VLAN numéro 50 (pour garder une cohérence avec le sous-réseau IP caractérisant ce réseau) et le nommer « Formation ». Affecter l'ensemble des ports de ces commutateurs au VLAN 50 (hormis le port de management).
Commutateur central : affectation du port qui relie le commutateur central au commutateur 4 au VLAN 50. Affecter le port qui relie le commutateur central au serveur DHCP en *trunk* (on ne peut pas le mettre en *access* sur le VLAN 50, sinon seul ce réseau pourra obtenir des configurations IP dynamique). Affecter le port qui relie le commutateur central au routeurLANG en *trunk* également.
Routeur : il faut créer une interface virtuelle appartenant au réseau 50. On pourra y apporter des ACL pour réglementer les communications selon les contraintes de sécurité du LAN (exemple le réseau 192.168.50.0 n'est pas autorisé à communiquer avec tous les autres réseaux internes mais avec l'hôte DHCP et serveur web).
Pour aller plus loin : on peut autoriser une segmentation logique totale, c'est-à-dire créer différents VLAN pour l'ensemble des sous-réseaux. On pourrait également admettre qu'il serait plus sécurisé de connecter le serveur web sur le routeur WAN.

2.3 Expliquez les tests que vous pouvez réaliser pour vérifier le bon fonctionnement de la séparation des postes utilisateurs à l'intérieur du réseau.

Il suffit d'envoyer un *ping* vers un autre réseau IP ou encore faire un *ping* vers l'adresse de diffusion : 192.168.50.255 (on verra ainsi le domaine de diffusion).
Il faut ensuite créer une demande DHCP d'un client de la salle de formation et réaliser une connexion http vers le serveur web. On peut également imaginer faire une demande de connexion à un réseau distant public (commande *tracert*). Il n'y aura pas de réponse mais on pourra observer si la demande traverse les routeurs.

Chapitre 6
Intégrer les enjeux liés aux cyberattaques et à l'obligation de protection des données

Missions professionnelles

1 Caractériser les risques liés à une utilisation malveillante d'un système informatique, p. 138

1. Indiquez pourquoi la confidentialité des données archivées n'est pas garantie par la procédure d'archivage utilisée par Cibeco.

Le serveur d'archivage est localisé dans une salle commune utilisée par les clients et les gérantes de Cibeco. En cas d'oubli de la clé USB sur le serveur, n'importe quel client pourrait la récupérer et accéder aux informations archivées. L'accès au serveur d'archivage n'a donc pas de sécurisation physique. De plus, les données archivées ne sont pas chiffrées n'en garantissant pas la confidentialité en cas d'acte malveillant. Enfin, en cas d'oubli de verrouillage de l'écran de veille, le délai de 5 minutes d'inactivité peut permettre à quiconque d'accéder aux archives.

2. Argumentez sur le risque lié à l'indisponibilité du serveur d'archivage de Cibeco compte tenu de la procédure d'archivage mise en place par l'entreprise.

Les données archivées sont stockées sur un seul serveur physique qui constitue ainsi un point unique de défaillance. Si ce serveur est compromis suite à un incident ou à une attaque, alors toutes les archives sont perdues. De plus, un client peut l'endommager étant donné qu'il est physiquement accessible.

3. Expliquez pourquoi la politique d'archivage de Cibeco n'est pas conforme au RGPD.

Le RGPD impose que des mesures de sécurité soient prises en adéquation avec le risque encouru compte tenu du caractère confidentiel des données stockées (article 32 du RGPD). Or, ce n'est pas le cas ici. En effet, l'absence de chiffrement et la non-séparation des serveurs des clients avec ceux de la pépinière sont incompatibles avec le minimum requis pour la sécurisation des données archivées.

4. Justifiez, pour chacun des risques, le niveau de gravité à sélectionner dans la liste déroulante du ticket de déclaration d'un d'incident.

Risque R1 : une personne malveillante accède frauduleusement aux données archivées.
→Niveau de gravité : maximal. En effet, il s'agit d'une brèche de confidentialité pouvant compromettre des données à caractère personnel (DCP).
Risque R2 : une personne malveillante modifie frauduleusement le contenu des données archivées.
→Niveau de gravité : maximal. En effet, l'intégrité des archives est compromise ce qui peut les rendre fausses et donc non valables.

2 Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité, p. 140

1. Recensez les conséquences techniques de l'attaque subie par Ecotri, en fonction des critères DIC (disponibilité, intégrité, confidentialité).

- **Disponibilité :** certaines fonctionnalités du site web du client Ecotri ne sont plus utilisables car leur contenu a été substitué par des messages malveillants. Ainsi, les informations de la page d'accueil ne sont plus disponibles.
- **Intégrité :** le contenu du site a été modifié.
- **Confidentialité :** les coordonnées des clients sont visibles sur la page d'accueil du site, or ce sont des informations confidentielles.

2. Indiquez, en argumentant, si ces conséquences peuvent affecter d'autres clients, compte tenu de la procédure utilisée par Cibeco pour le développement Web de ses formulaires.

Cibeco utilise la même procédure pour développer les formulaires de ses clients (document 3). Or cette procédure ne vérifie pas le contenu des données saisies. Du code malveillant peut ainsi être injecté lors de la saisie, affectant d'autres clients qui disposent de ces mêmes formulaires développés par Cibeco.

3. Relevez les conséquences humaines et financières de cette attaque pour Ecotri.

L'extrait des commentaires sur les réseaux sociaux montre des conséquences :

- sur le plan humain : détresse du gérant d'Ecotri, stress, panique, perte de moyens ;
- sur le plan financier : fuite des clients qui résilient leur abonnement, risque de chute du chiffre d'affaires.

4. Identifiez les conséquences juridiques possibles pour l'auteur de l'attaque. L'adresse IP de l'attaquant peut-elle être identifiée ?

La fiche CEJM 7 précise les infractions et les sanctions encourues. Pour l'attaque du site web du client Ecotri, il s'agit d'un accès illégitime à un système de traitement automatisé qui est puni de deux ans d'emprisonnement et de 30 000 € d'amende.
L'adresse IP de l'auteur de l'attaque est visible dans les journaux systèmes (document 5).

3 Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation, p. 143

1. Identifiez, en argumentant, les obligations légales non respectées par Cibeco en matière de sécurisation physique des archives.

- Extincteurs uniquement dans les salles communes : la salle des serveurs n'est donc pas protégée.
- Conservation des archives sur clé USB alors que c'est un support de conservation non recommandé.
- Pas de vidéoprotection et pas de câble d'antivol : le serveur est physiquement accessible et peut être ouvert afin que son disque soit dérobé.
- Copie des archives seulement une fois par semestre. Si un problème se produit avant la copie, il y a donc une perte des données.

2. La procédure de traçabilité des accès aux archives de Cibeco est-elle conforme à la réglementation ?

La traçabilité des accès aux archives est gérée par un formulaire papier. Or le document 2 montre que ce formulaire n'est pas à jour. En effet, la trace de la dernière consultation n'y figure pas. Cette procédure n'est donc pas conforme à la réglementation qui impose une véritable traçabilité par des moyens automatisés permettant d'imputer un accès à une personne physique à une date donnée.

3. Expliquez en quoi Cibeco ne respecte pas les obligations légales en matière de protection des données stockées sur son serveur de base de données nommé miRDB.

L'accès au serveur miRDB nécessite une authentification. Or la page d'authentification n'est pas chiffrée comme l'atteste le message d'avertissement du navigateur (document 3). Cibeco se doit pourtant de mettre en place un niveau de sécurité en relation avec les données stockées et le risque encouru. Ce n'est pas le cas ici car le serveur miRDB contient des données confidentielles sur les transactions financières de Cibeco.

4. Indiquez si la mise en place d'un mot de passe fortement sécurisé pour l'accès au serveur miRDB suffit à corriger les manquements légaux précédemment relevés.
Justifiez votre réponse.

Non, la mise en place d'un mot de passe fortement sécurisé, bien qu'indispensable, ne suffit pas. En effet, même solide, un mot de passe peut être capturé par un attaquant si la connexion n'est pas chiffrée (écoute clandestine).

Travaux en laboratoire informatique

Protéger une application Web en appliquant un codage sécurisé, p. 145

ÉTAPE 1 La préparation de l'environnement de travail

1. Vérifiez que votre ordinateur dispose d'au minimum 6 Go de mémoire vive. Ensuite, téléchargez puis installez le logiciel VirtualBox.

Cette vérification peut se faire en consultant les paramètres de la machine. Par exemple, sous Windows, il faut ouvrir l'explorateur de fichiers pour faire un clic droit sur « Ce PC » puis cliquer sur « Propriétés » afin d'afficher la quantité de mémoire vive disponible. Sous linux, il est possible d'utiliser la commande free -h. Pour installer VirtualBox, il faut suivre la fiche méthode 3, p. 207.

2. Téléchargez le fichier DELAGRAVE-LAB-THEM4.ova. Il contient les quatre machines du laboratoire, avec tous les logiciels nécessaires aux manipulations.

Il faut utiliser le lien indiqué dans le livre pour télécharger le fichier. ova.

3. Effectuez un clic droit sur ce fichier puis cliquez sur « Ouvrir avec Virtual VM Box » afin d'importer ces machines dans votre logiciel VirtualBox.

Il est aussi possible de double-cliquer sur le fichier afin de lancer l'import des machines virtuelles.

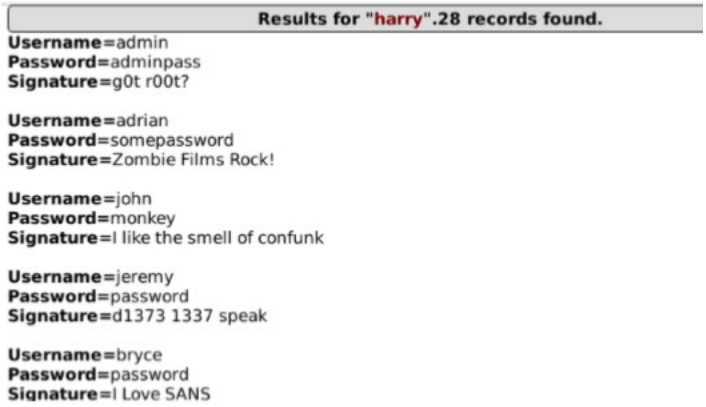
4. Démarrez la machine DELAGRAVE-CLIENT-LEGITIME-UBUNTU. Ensuite, suivez les instructions indiquées dans la vidéo nommée LAB-THEME4-CONFIG. mkv présente sur le bureau de cette machine afin d'initialiser les cartes réseaux des quatre machines. Enfin, démarrez toutes les machines.

Pour démarrer une machine virtuelle, il suffit de double-cliquer dessus ou de cliquer sur le bouton « démarrer » dans VirtualBox. Il peut être intéressant de faire un *snapshot* (instantané) de chaque machine avant de commencer le travail. Ainsi, en cas d'incident, il sera possible de revenir à l'état original des machines. Pour faire un *snapshot*, il faut suivre la fiche méthode 3, p. 207.

ÉTAPE 2 La réalisation d'une attaque de type injection SQL

5. Réalisez l'injection SQL en suivant les instructions figurant dans le fichier LAB-THEME4CHAP6-DEFI. txt présent sur le bureau de la machine DELAGRAVE-CLIENT-HACKER-UBUNTU. Que constatez-vous ?

La page cible sur Mutillidae est *user-info.php*. Lorsque l'injection est réalisée, la liste de tous les membres du site s'affiche ce qui constitue une brèche de confidentialité.
Lors de la saisie du code SQL dans les champs, il faut faire attention aux espaces.
Remarque : il peut être opportun de prolonger cette question avec un rappel sur les tables de vérités avec les opérateurs AND et OR.



ÉTAPE 3 La contre-mesure de codage sécurisé

6. Positionnez le niveau de sécurité à 5 sur Mutillidae, puis reproduisez les étapes permettant de réaliser l'injection SQL. Que constatez-vous ?

Lorsque le niveau de sécurité 5 est activé, l'attaque est un échec. En effet, le code exécuté est différent et intègre des vérifications de sécurité. La page concernée est toujours user-info.php.

7. Comparez le code source de la page user-info.php dans sa version sécurisée et dans sa version non sécurisée. Quelle partie du code permet d'éviter l'injection SQL ? Que pouvez-vous en déduire en matière de bonnes pratiques de codage sécurisé ?

Lorsque le codage sécurisé est activé, deux types de vérifications de sécurité sont effectués :

- la vérification de la longueur des données saisies ;
- la vérification de la présence de caractères suspects typiques des injections SQL.

En effet, une longueur trop importante est suspecte et peut correspondre à l'injection de code SQL malveillant. Il convient donc de limiter cette longueur côté client et côté serveur.
Quant aux caractères suspects, il faut les vérifier via la constitution d'une liste noire de caractères interdits. Ces vérifications ne sont pas effectuées en cas d'activation du codage non sécurisé.
La partie du code qui permet d'éviter les injections SQL est la suivante :

```
var lUnsafeCharacters = /[`~!@#$%^&*()-_=+\[\]{}\\|;':",./<>?]/;

if(lValidateInput == "TRUE"){
        if (theForm.username.value.length > 15 ||
                theForm.password.value.length > 15){
                        alert('Username too long. We dont want to allow
                        return false;
        }// end if

        if (theForm.username.value.search(lUnsafeCharacters) > -1 ||
                theForm.password.value.search(lUnsafeCharacters) > -1){
                        alert('Dangerous characters detected. We can\'t
                        return false;
```

Concernant les bonnes pratiques de codage, il convient de toujours vérifier les données saisies par un utilisateur dans un formulaire.

Applications

1 QCM, p. 157

1. L'archivage intermédiaire :

☐ correspond à la base des informations en cours d'utilisation.
☒ peut comporter des données issues de transactions réalisées avec des cartes bancaires.
☒ nécessite d'être attentif à la durée maximale de conservation des données.

2. Quels sont les supports numériques recommandés pour un archivage pérenne des données ?

☒ Un disque dur
☐ Un DVD
☒ Une bande magnétique
☐ Une clé USB
☐ Des papiers dans des boîtes en carton

3. Quelles sont les affirmations exactes concernant l'archivage ?

☐ L'archivage est la duplication des données en cours de traitement en vue de pouvoir les restaurer.
☒ L'archivage est la copie d'anciennes données qui ne sont plus en cours de traitement à des fins de conservation.
☒ Des mesures appropriées doivent être mises en œuvre pour assurer la confidentialité des archives.

4. Le protocole HTTP :

☐ assure la confidentialité des échanges.
☐ assure l'intégrité des échanges.
☒ n'est pas un protocole sécurisé.

5. Les journaux systèmes (*logs*) :

☒ sont un moyen d'obtenir des preuves en cas d'attaque informatique.
☒ nécessitent de disposer de suffisamment d'espace disque pour être conservés.
☐ sont à conserver sans limitation de durée.

6. Jean veut envoyer un message confidentiel à Déborah. Quelles sont les affirmations exactes ?

☐ Jean chiffre le message avec sa clé privée et Deborah déchiffre le message avec sa clé publique.
☐ Jean chiffre le message avec sa clé publique et Deborah déchiffre le message avec sa clé privée.
☒ Jean chiffre le message avec la clé publique de Deborah et Deborah déchiffre le message avec sa clé privée.

7. Le chiffrement symétrique :

☐ utilise une paire de clés et garantit l'authenticité de l'expéditeur.
☒ utilise une seule clé pour chiffrer et déchiffrer le message.
☐ utilise une seule clé et nécessite le recours à une autorité de certification.

8. La méthode d'authentification SSO :

☐ permet d'utiliser plusieurs mots de passe pour accéder à différents services.
☒ permet à une personne d'utiliser un seul mot de passe pour accéder à de multiples services au sein de l'entreprise.
☐ permet d'accéder à un seul et unique service.

9. Une attaque de type injection SQL :

□ consiste à saturer un site web en envoyant des millions de requêtes.

☒ consiste à injecter du code SQL dans un champ de formulaire vulnérable.

□ peut permettre de pirater le compte d'un utilisateur légitime.

10. La loi Godfrain du 5 janvier 1988 :

☒ est antérieure à la loi sur la confiance dans l'économie numérique.

□ permet l'harmonisation des législations des États membres de l'UE.

☒ réprime les actes de criminalité informatique et de piratage.

2 Comprendre les enjeux liés à l'archivage des données, p. 158

1. Relevez les principaux enjeux associés à l'archivage numérique.

- **Enjeu d'efficacité : accès facile et rapide**

Il s'agit de pouvoir accéder rapidement à l'information recherchée en identifiant la version validée d'un document archivé.

- **Enjeu de sécurité : prise de décisions**

La consultation de données archivées fiables et non manipulées permet de prendre des décisions. Ces décisions peuvent être non pertinentes en cas d'archives falsifiées.

- **Enjeu technologique : système informatique fiable**

L'harmonie entre les systèmes matériels et logiciels permet de garantir un archivage pérenne.

2. Indiquez quels sont les domaines d'un système d'information mobilisés lors de la mise en œuvre d'une procédure d'archivage numérique.

- **Gestion et recherche documentaire**

Capacité de rechercher des données archivées via des moteurs de recherche. Cette recherche peut être facilitée par des bases de connaissances et des outils sémantiques. Une base de connaissance regroupe des connaissances dans un domaine spécialisé. Il est par exemple possible de mémoriser les dernières recherches effectuées par un utilisateur dans les archives afin de permettre un accès plus rapide lors d'une prochaine recherche similaire.

- **Gestion de la preuve et de la sécurité**

Les données archivées doivent être exactes et n'avoir fait l'objet d'aucune corruption.
Les mécanismes de signatures numériques et de contrôle d'intégrité sont utilisés conjointement avec un mécanisme d'horodatage fiable.

- **Gestion des outils et des infrastructures de stockage**

Utilisation de supports d'archivage pérennes avec des infrastructures de stockage et des outils de conservation adaptés : salle sécurisée, redondance, supports adaptés tels que des bandes magnétiques ou des disques durs.

3. Pourquoi la mise en place d'une veille technologique sur les supports d'archivage est-elle nécessaire ? Justifiez votre réponse.

La veille technologique est un processus qui consiste à s'informer sur l'évolution des outils et des techniques disponibles dans un domaine étudié.
Un système d'archivage repose en grande partie sur le choix de bons supports. En effet, ces supports vieillissent et évoluent : obsolescence des technologies, amélioration des fonctionnalités de certains supports. C'est en réalisant une veille technologique sur ces supports que le responsable des archives peut garantir une conservation pérenne en adéquation avec les évolutions technologiques (compatibilité avec les systèmes disponibles, durée de vie, méthode de maintenance, amortissement…).

3. Identifier les risques liés à une procédure d'authentification, p. 159

1. Recherchez des informations sur Internet afin d'expliquer en quoi consiste un certificat de sécurité.

Un certificat de sécurité est une carte de visite numérique utilisée pour identifier et authentifier une personne ou un serveur. Ce certificat contient des informations sur la personne ou le serveur ainsi que la clé publique correspondante. La clé privée n'est pas présente dans le certificat et doit être conservée par son propriétaire (identité numérique complète).

2. Expliquez le message d'avertissement qui apparaît dans le courriel (annexe).

Le message indique que le certificat de sécurité n'est pas approuvé. Cela signifie que les entités racines publiques présentes dans le navigateur n'ont pas signé ce certificat. Par conséquent, le navigateur émet un message d'avertissement.

3. Relevez, en justifiant, les risques encourus lors de l'authentification d'un membre sur ce site.

Le certificat n'étant pas approuvé, il y a un risque d'usurpation d'identité et d'écoute clandestine. En effet, un attaquant peut se faire passer pour le serveur de *SortieFacile* et récolter les identifiants de connexion saisis par un visiteur. Dans ce cas, l'attaquant réalise une copie falsifiée du site de *SortieFacile* et présente un certificat illégitime. La victime peut ainsi voir son compte piraté. De plus, le pirate peut avoir accès aux données confidentielles liées au compte de la victime (liste de contacts, liste de sorties, préférences…).

4. Relevez les options proposées par le navigateur suite à l'affichage de ce message d'avertissement. Que pouvez-vous conclure concernant l'option à appliquer ?

Le navigateur propose deux options :

- Continuer avec ce certificat : cette option n'est pas recommandée dans le contexte d'un site internet en production avec saisie d'identifiants de connexion. En effet, un site web en production sérieux doit proposer un certificat à jour et connu des autorités racines. L'internaute peut tout de même poursuivre à ses risques et périls en acceptant ce certificat.
- Abandonner la connexion : l'internaute tient compte du message d'avertissement et abandonne la connexion. Cette option est fortement recommandée dans ce cas.

4. Caractériser les conséquences d'une fraude informatique, p. 160

1RE PARTIE Les principales fraudes informatiques

1. Rendez-vous sur le site cybermalveillance.gouv.fr et cliquez sur « Accéder au kit ».

Le kit peut se télécharger via le lien suivant : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation

2. Visionnez les vidéos associées à chacune des fraudes : hameçonnage, arnaque au faux support technique, rançongiciels. Complétez ensuite ce tableau.

Fraudes	Descriptions	Conséquences
Hameçonnage	Fraude visant à obtenir des informations confidentielles via des liens renvoyant vers des copies de sites falsifiées. La fraude se réalise généralement par l'envoi de mails massifs plus ou moins ciblés contenant des liens malveillants. La victime croit s'adresser à un tiers de confiance.	Récupération des identifiants de connexion de la victime (*login* et mot de passe, numéros de carte de crédit, numéro ou photocopie de la carte nationale d'identité).
Arnaque au faux support technique	Un message alarmiste d'un faux support technique demande à une victime de fournir ses identifiants de connexion afin de réaliser une opération de maintenance urgente : menace de désactivation ou de suppression de compte, menace de suppression de données en cas de refus.	Récupération des identifiants de connexion de la victime. Par la suite, usurpation d'identité et vol d'informations et de numéros de carte de crédit, achats réalisés avec le compte de la victime.
Rançongiciels	Un logiciel malveillant chiffre le disque de la victime. Le fraudeur demande une rançon en contrepartie du déchiffrement.	Perte d'argent et d'informations en cas d'absence de politique de sauvegarde efficace.

2E PARTIE Un jeu pour comprendre la fraude de type « arnaque au président »

3. Visionnez la vidéo, puis expliquez en quoi consiste la fraude présentée.

Un fraudeur se fait passer pour un décideur (chef de service, comptabilité) et demande qu'une opération soit réalisée (virement, fourniture de documents confidentiels…).
Un fraudeur habile s'est renseigné sur les habitudes du décideur (langage utilisé, collaborateurs concernés) afin d'accroître sa crédibilité. Il s'agit d'une attaque de type ingénierie sociale et manipulation.

4. Expliquez le risque financier qui pèse sur l'entreprise cible.

Si la victime n'est pas prudente, elle peut réaliser l'opération demandée et l'entreprise peut ainsi perdre beaucoup d'argent. Soit parce qu'un virement frauduleux a été réalisé ou parce qu'une entreprise a divulgué des informations sur une innovation en cours causant ainsi une perte potentielle de brevet.

5. Classez ce risque en fonction du niveau de gravité et de vraisemblance.

Le niveau de gravité est très important compte tenu des conséquences possibles : risque financier, réputation entamée de l'entreprise victime, perte de savoirs confidentiels. Concernant le niveau de vraisemblance, beaucoup d'entreprises peuvent être victimes de cette fraude. Un fraudeur habile et bien renseigné peut réaliser ce type de fraude en utilisant simplement un téléphone. Donc le niveau de vraisemblance est important.

6. Les informations sur l'entreprise cible ont-elles été obtenues de manière légale ? Justifiez votre réponse.

Oui car, malheureusement, de simples recherches sur Internet peuvent suffire pour obtenir ces informations. Les réseaux sociaux sont souvent une source d'information permettant de préparer ce type d'attaque. Trop de professionnels mélangent leur vie privée et leur vie professionnelle ce qui fournit aux attaquants des informations exploitables obtenues légalement.

7. Quelle sanction encourt l'auteur de la fraude ?

Dans le cadre d'une escroquerie, l'auteur de la fraude risque une peine de cinq ans d'emprisonnement et de 375 000 € d'amende, d'après l'article 313-1 du Code pénal.

Chapitre 7
Archiver et protéger les données et les preuves numériques

Missions professionnelles

1 Organiser la collecte et la conservation des preuves numériques, p. 162

1. Montrez, en développant chaque argument, que Cibeco dispose des moyens techniques permettant d'appliquer les recommandations d'usage en matière de collecte des preuves numériques.

- Centralisation des journaux systèmes afin d'éviter les incohérences entre les différents points de collecte.
- Présence de deux serveurs pour la collecte afin de prévenir une panne sur un serveur (grappe de deux serveurs redondés), donc tolérance de panne.
- Présence d'un serveur de temps donc horodatage correct.
- Collecte via un VLAN dédié.
- Bande passante garantie pour le transit des journaux systèmes.
- Consultation des journaux systèmes facilitée par une interface web.

2. Relevez les événements collectés par les journaux systèmes de Cibeco et vérifiez que cette liste est bien complète.

Le document 2 donne la liste des évènements collectés : authentification sur les serveurs, accès aux ressources, activités des programmes et des systèmes (arrêts, redémarrages…).
Le document 3 montre les catégories d'événements susceptibles de lever des alertes enregistrées dans les journaux. Cette liste comprend des évènements de type information ainsi que des alertes pouvant être liées à des actes malveillants (tentative de force brute).
Cette liste est bien conforme aux recommandations de l'ANSSI présentes dans le paragraphe 2 de la fiche savoir technologique 11 sur la notion de traçabilité.

3. Montrez que chacun des supports de stockage utilisé par Cibeco permet de conserver durablement les preuves collectées.

- Conservation sur bandes magnétiques et non sur clé USB : support de conservation durable.
- En amont, enregistrement sur des disques durs configurés en RAID 5 afin d'assurer une tolérance de panne.

Le nombre de bandes utilisées (10) ainsi que leur capacité de stockage (10 To) avec une copie en double devrait permettre d'éviter les problèmes liés à des capacités de stockage insuffisants (voir document 5).

4. Le lieu choisi par Cibeco pour conserver ses preuves numériques doit permettre de faire face à des sinistres importants. Citez les éléments qui en attestent.

La baie qui sert pour le stockage des preuves numériques comporte les dispositifs suivants :

- système anti-incendie ;
- copie en double ;
- climatisation en cas de canicule.

Ces mesures permettent de faire face à des sinistres et peuvent être complétées par un stockage des archives dans un second bâtiment (cf. document 6).

2 Appliquer les procédures garantissant le respect des obligations légales, p. 166

1. Indiquez, en argumentant, si la procédure prévue par Cibeco pour faire face à la brèche de sécurité mentionnée dans la FRAP n° 1 garantit le respect des obligations légales.

- En cas de perte ou de vol de l'ordinateur portable de la gérante, sa clé d'accès doit être révoquée. La FRAP ne fait pas mention de révocation de clé.
- Le disque dur n'est pas chiffré. En cas de vol, les données peuvent être accessibles.
- Les données confidentielles ne sont pas effacées de manière sécurisée ce qui peut permettre à l'auteur d'un vol de les restaurer.

Le niveau de sécurité lié la FRAP n° 1 est insuffisant et n'est pas conforme au niveau requis par les obligations légales compte tenu des données manipulées (DCP).

2. Expliquez en quoi la procédure prévue par Cibeco pour faire face à la brèche de sécurité mentionnée dans la FRAP n° 2 ne garantit pas la confidentialité et l'intégrité des journaux systèmes exigées par la loi.

- Absence de chiffrement lors du transfert des journaux systèmes des disques vers les bandes magnétiques, donc écoute clandestine possible.
- Absence de vérification des sommes de contrôles (*hash*). L'intégrité des journaux systèmes n'est pas garantie durant leur transfert. Leur validité, en tant que preuve numérique, peut être remise en cause.

3. Montrez que la procédure technique prévue par Cibeco pour faire face à la brèche de sécurité mentionnée dans la FRAP n° 3 ne suffit pas à garantir l'intégrité des applications Web des clients prévue dans l'accord de niveau de service.

- Sauvegarde des pages web des clients une fois par trimestre seulement. En cas de besoin de restauration, il y a donc un risque important que la sauvegarde ne couvre pas totalement la perte des données. Il faudrait une sauvegarde quotidienne.
- Sauvegarde de la base de données largement insuffisante car une fois par trimestre. Les données comportant des flux de clientèle, doivent être sauvegardées beaucoup plus fréquemment ou via l'utilisation d'un système de réplication en temps réel.

L'intégrité des applications web des clients n'est donc pas garantie en cas de panne importante d'un serveur Web ou de sa base de données.

4. Expliquez pourquoi les organismes de lutte contre la cybercriminalité exigent que ces procédures garantissent le respect des obligations légales.

En cas d'action judiciaire, les preuves doivent être valables. Si la confidentialité, l'intégrité et la disponibilité des preuves numériques ne sont pas assurées, les preuves numériques collectées risquent d'être invalidées.

Travaux en laboratoire informatique

Organiser la collecte des preuves numériques, p. 169

ÉTAPE 1 : La préparation de l'environnement de travail

1. Préparez votre environnement de travail en suivant les étapes décrites dans le document 1, puis démarrez toutes les machines.

Il faut reprendre le travail en laboratoire du chapitre 6. Toutes les machines doivent être démarrées et leur adressage IP doit être configuré.

2. Connectez-vous au pare-feu en suivant les étapes décrites dans le document 2.

La connexion au pare-feu se fait depuis le navigateur via une interface Web en HTTPS. Il faut saisir l'URL suivant : *https ://192.168.50.254* et accepter le certificat présenté (certificat d'usine). La connexion se fait via le login *admin* et le mot de passe par défaut *pfsense*. Une fois la connexion validée, le tableau de bord du pare-feu s'affiche.

ÉTAPE 2 : La configuration du serveur de temps sous pfsense

3. Mettez votre pare-feu pfSense à l'heure.

Il faut cliquer sur « System » puis sur « General Setup ». Ensuite, dans la rubrique de localisation, sélectionner la zone géographique « Europe/Paris », puis valider en cliquant sur « Save ». Attention, il faut que le pare-feu dispose d'une connexion à internet.

4. Configurez votre pare-feu pfSense pour qu'il soit un serveur de temps.

Cliquer sur le menu « Services » puis sur « NTP ». Il faut ensuite sélectionner les interfaces « lan-in » et « srv-in » sur lesquelles le serveur de temps va écouter les requêtes des clients. Les autres paramètres peuvent garder leur valeur par défaut. Terminer en cliquant sur le bouton « Save ».

5. Mettez le serveur Web Mutillidae à l'heure en vous appuyant sur le serveur de temps pfSense.

Il faut ouvrir le fichier ntp.conf situé sur le serveur web Mutillidae via la commande suivante : « sudo nano /etc/ntp.conf ».
Ensuite, dans ce fichier, localiser les lignes commençant par pool et les remplacer par la seule ligne suivante :
server 172.16.10.254
172.16.10.254 est l'adresse IP du pare-feu du côté de la zone serveur (passerelle des serveurs).
Enfin, fermer le fichier puis redémarrer le service ntp avec la commande suivante : « service ntp restart ». La commande « ntpq -pn » permet de vérifier que la configuration est correcte.

ÉTAPE 3 : La configuration de l'enregistrement des traces

6. Configurez votre pare-feu pfSense pour qu'il enregistre les traces des connexions du hacker sur le serveur Web Mutillidae.

Il faut cliquer sur le menu « Firewall » puis sur l'interface « lan-in ». Ensuite, cliquer sur l'icône permettant de modifier la deuxième règle. En effet, c'est cette règle qui autorise la zone cliente (à laquelle appartient le hacker) à se connecter au serveur Web Mutillidae. Lorsque la règle est en mode édition, il suffit de cocher la case permettant de journaliser les paquets gérés par cette règle puis de valider en cliquant sur le bouton « Save » puis sur le bouton « Apply Change ».

7. Connectez-vous au serveur Web Mutillidae depuis la machine du hacker, puis vérifiez que le pare-feu trace votre connexion dans les journaux systèmes.

- **Étape n° 1**

Depuis la machine du hacker, ouvrir un navigateur puis se connecter au serveur Web Mutillidae en saisissant l'URL suivant : http ://172.16.10.5/mutillidae. Ensuite, naviguer sur quelques pages de l'application. Le pare-feu enregistre les traces des connexions.

- **Étape n° 2**

Se connecter au pare-feu (https ://172.16.10.254) ensuite cliquer sur le menu « Firewall » puis sur l'interface « lan-in ». Il ne reste plus qu'à consulter les traces en cliquant sur l'icône des journaux systèmes situé en haut à droite de l'écran. Il est possible de réaliser un filtre de recherche en saisissant l'adresse IP du hacker. Les traces de connexion du hacker s'affichent.

Applications

1 QCM, p. 177

1. Quelles sont les informations exactes concernant le PRA et le PCA ?

☒ Le PRA permet d'assurer la reprise des activités en cas de sinistre important.
□ Le PCA permet d'assurer l'intégrité d'une preuve numérique.
☒ Le PCA permet d'assurer une continuité des activités de l'entreprise en cas d'incident.

2. La rotation des journaux systèmes :

□ nécessite le recours à plusieurs salariés de l'entreprise.
☒ automatise la permutation et la suppression des journaux systèmes selon des intervalles de temps définis.
□ est un processus qui augmente la capacité de stockage des disques.

3. Quels sont les organismes de lutte contre la cybercriminalité ?

☒ BEFTI
☒ OCLCTIC
□ BGP

4. Un serveur de temps :

☒ synchronise les horloges des machines du réseau informatique.
□ assure l'intégrité des échanges.
□ distribue des adresses IP aux machines du réseau.

5. Les sommes de contrôles (*hash*) garantissent :

☒ l'intégrité.
□ la confidentialité.
□ la disponibilité.

6. Les FRAP sont :

☒ des feuilles d'analyse associées à un audit technique.
☒ des documents remplis lors de la détection d'un dysfonctionnement ou d'un risque.
□ des feuilles d'analyse contenant tous les journaux système.

7. Quels sont les algorithmes de calcul de sommes de contrôles (*hash*) ?

☒ SHA256
☒ MD5
□ SNMP
□ CBQ

8. L'algorithme de chiffrement AES :

☒ est un algorithme récent et robuste.
□ assure la disponibilité d'une ressource.
□ permet d'accéder à un seul et unique service.

9. Le protocole NTP :

□ signifie *Network Transfert Protocol*.
□ permet de chiffrer les échanges.
☒ permet de disposer d'un serveur de temps.

10. Concernant la collecte des preuves numériques, l'ANSSI recommande :

☒ de disposer d'un espace disque suffisant, redondé et supervisé.
☒ de collecter les traces en temps réel.
□ d'autoriser tous les utilisateurs de l'entreprise à consulter tous les journaux systèmes.
□ d'interdire le chiffrement des journaux systèmes.

2 Utiliser les journaux systèmes comme preuves numériques, p. 178

CAS N° 1

1. Indiquez si ce cas relève d'un acte malveillant. Justifiez votre réponse.

Non, ce cas ne relève pas d'un acte malveillant mais d'un problème lié à des flux qui ralentissent les accès réseaux (bande passante).

2. Expliquez en quoi la consultation des journaux systèmes a permis d'améliorer le fonctionnement du réseau informatique de l'établissement.

Les journaux systèmes indiquent la date et l'heure des évènements tracés. Or, l'administrateur a relevé les heures des ralentissements observés et analysé les flux concernés dans les journaux systèmes. Cette analyse a permis d'en déduire que les flux du gestionnaire de parc sont la cause des ralentissements observés. Les mesures prises par la suite ont permis d'améliorer le fonctionnement du réseau informatique.

CAS N° 2

3. Indiquez si ce cas constitue une brèche de confidentialité sur les données à caractère personnel. Justifiez votre réponse.

L'usurpation de compte décrite dans le document permet d'accéder aux informations associées à ce compte. Or ces informations peuvent être des données à caractère personnel (nom, prénom, date de naissance…). Il s'agit donc bien d'une brèche de confidentialité.

4. Donnez le nom de l'organisme chargé d'enquêter. Indiquez qui est le responsable juridique du système d'information.

La gendarmerie nationale est chargée d'enquêter dans le cas présenté. Le responsable juridique du système d'information est le chef d'établissement (proviseur).

5. Justifiez la nécessité de consulter les journaux systèmes pour aider à la résolution de ce cas.

Les journaux systèmes pourraient prouver, par exemple, que le propriétaire du compte était connecté sur un autre système et dans une autre salle au moment de la réalisation des faits ce qui l'innocenterait.

3 Exploiter des preuves numériques, p. 179

1. Rappelez quel est le rôle de l'OCLCTIC dans le cadre de cette affaire.

L'OCLCTIC est l'organisme de police nationale chargé d'enquêter sur les affaires de cybercriminalité. Le cas présent est bien associé à une affaire de cybercriminalité.

2. À l'aide de recherches sur Internet, définissez les termes suivants : métadonnées, données EXIF, géolocalisation.

- **Métadonnées :** donnée servant à décrire ou définir une autre donnée. Par exemple, pour une photo, on peut citer la date de prise de la photo ou les coordonnées GPS du lieu de prise de la photo.
- **Données EXIF :** *Exchangeable image file*. Ensemble de données relatives à chaque photo et présentées dans un format normalisé. Ces données sont gérées par l'appareil photo lors de la prise de vue.
- **Géolocalisation :** procédé permettant de positionner un objet, un véhicule ou une personne sur un plan ou une carte à l'aide de ses coordonnées GPS.

3. Rendez-vous sur le site GitHub, qui contient des exemples d'images permettant de réaliser des tests pour retrouver des métadonnées.

Ouvrir un premier onglet sur le navigateur et se rendre sur le site en question.

4. Ouvrez un autre onglet sur le navigateur et rendez-vous sur le site metapicz.com.

Ouvrir un deuxième onglet sur le navigateur puis se rendre sur le site en question.

5. Téléchargez une image depuis le site GitHub et importez-la dans la zone d'analyse du site metapicz.com.

L'image à télécharger servira pour faire des analyses via le site metapicz.com.

6. Relevez les métadonnées disponibles et testez à nouveau avec une autre image.
Pour chaque image, vérifiez si les informations suivantes sont disponibles : auteur de l'image, géolocalisation, appareil photo utilisé.

Tout dépend de l'image téléchargée. Il est possible que certaines images ne permettent pas d'obtenir toutes ces informations. On peut envisager de demander aux étudiants de récupérer une image prise depuis leur smartphone à des fins d'analyse. L'objectif de la question est de montrer que les paramètres par défaut des appareils photos (smartphones compris) peuvent enregistrer ce type d'information.

7. Expliquez l'intérêt de l'outil testé dans le cadre de l'enquête en cours.

Les données EXIF peuvent indiquer que l'appareil a été utilisé ainsi que le lieu, la date et l'heure de prise vue, ce qui peut compromettre l'auteur de la photo d'origine.

4 Collecter des preuves numériques, p. 180

1. Rendez-vous sur le site https://www.sophos.com, puis cliquez sur le lien permettant d'accéder aux démonstrations en ligne.

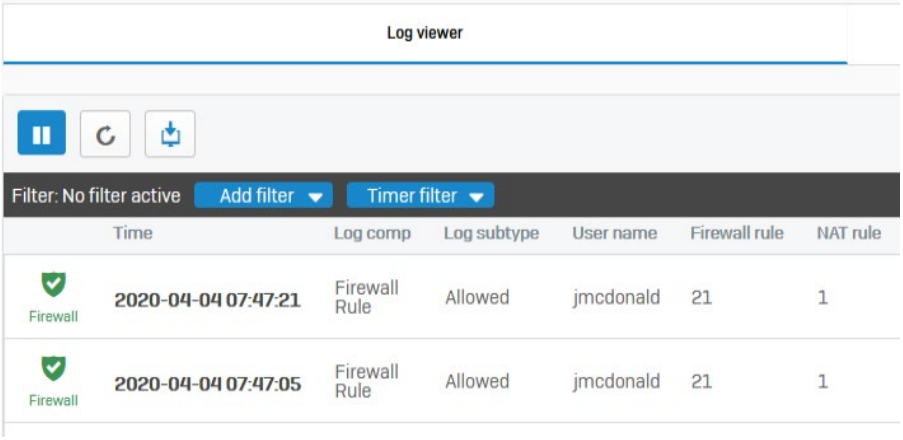
En cas de changement de lien sur le site de sophos, il est possible d'accéder à la démonstration en utilisant le lien suivant : *demo.sophos.com*.

2. Cliquez sur le bouton permettant d'accéder au pare-feu en ligne XG.
Ensuite, créez un compte afin d'accéder à la démonstration en ligne. Une fois le compte validé, connectez-vous en utilisant *demo* pour le login et pour le mot de passe.

Login = demo
Password = demo

3. Une fois connecté(e) au pare-feu, cliquez sur le bouton « log viewer » situé en haut, à droite. Une nouvelle fenêtre s'ouvre et affiche les traces des connexions qui transitent par le pare-feu.

La fenêtre suivante s'affiche après avoir cliqué sur le bouton « Log viewer » :



4. Relevez les noms des colonnes du tableau de synthèse des journaux systèmes. Expliquez le rôle de chaque colonne.

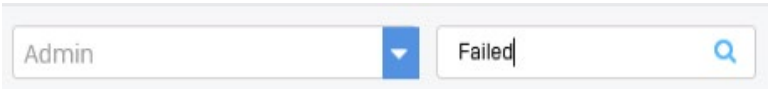
- **Time :** l'heure de l'événement enregistré dans les journaux systèmes.
- **Log comp** : type d'événement enregistré (règle de pare-feu, trafic invalide…).
- **Log subtype :** détail de l'action décrite dans les journaux systèmes (refus, acceptation…).
- **User name :** utilisateur concerné.
- **Firewall rule :** numéro de la règle de filtrage concernée.
- **NAT rule :** numéro de la règle de NAT concernée (traduction d'adresses).
- **In interface :** interface d'entrée du flux concerné.
- **Out interface :** interface de sortie du flux concerné.
- **Src Ip :** adresse IP source du flux concerné.
- **Dst Ip :** adresse IP de destination du flux concerné.
- **Scr Port :** port source du flux concerné.
- **Dst Port :** port de destination du flux concerné.

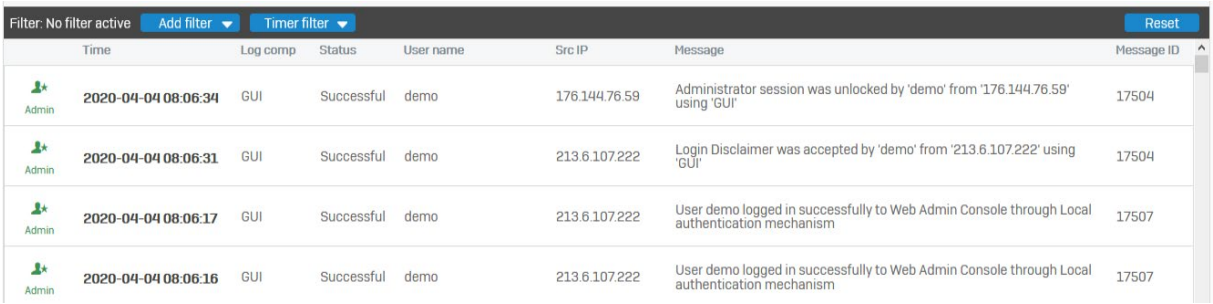
5. Cliquez sur la liste déroulante située en haut, à droite, puis relevez les catégories d'événements tracés par le pare-feu. Cette liste de catégories d'événements tracés est-elle en conformité avec ce que recommande l'ANSSI ?

Cette liste de catégories est complète et en conformité avec ce qui est recommandé par l'ANSSI. Il faut se référer à la fiche savoirs technologiques 11, p. 173 pour le vérifier :

- Authentification (présent dans la liste) ;
- Gestion des comptes et des droits (liée à l'authentification, email et compte admin) ;
- Accès ou modification des ressources et des configurations (rubrique System) ;
- Activité des processus et des systèmes (rubriques IPS, Firewall, Application filter…).

6. Dans la liste déroulante, sélectionnez la rubrique « Admin », puis saisissez la chaîne de caractères « Failed » dans la zone de recherche située à droite de la liste déroulante. Validez la saisie, puis expliquez à quoi correspond le résultat affiché et quel peut être son intérêt dans le cadre de la traçabilité des événements.





Le résultat affiché indique des traces associées à des échecs d'authentification avec le compte admin. Cela peut alerter sur des tentatives de force brute pour trouver le mot de passe du compte administrateur du pare-feu.

Évaluation 4

Missions

Analyser la sécurité du site extranet de Fermabio, p. 182

1.1. Expliquez pourquoi le test n° 1 montre que la confidentialité et l'intégrité ne sont pas garanties.

Le test n° 1 montre qu'une vulnérabilité de type XSS a été détectée. Ce type de vulnérabilité concerne le champ *commentaire_commande* du panier client et peut permettre à un pirate de récupérer le cookie d'identification d'un client.
Avec ce cookie, le pirate peut se connecter au compte du client ce qui constitue une brèche de confidentialité.
De plus, le pirate peut injecter du code javascript malveillant et ainsi modifier le contenu de la base de données, ce qui remet en cause l'intégrité des données stockées.

1.2. Proposez une modification de ce code source afin de corriger la vulnérabilité détectée.

Il faut repartir du document 2 contenant l'extrait de code non sécurisé et augmenter ce code avec la fonction *htmlspecialchars* décrite dans le rapport associé au test n° 1. La ligne à ajouter est en gras.

```
1 – < ? php
2 – //1 – Récupération du commentaire saisi par l'utilisateur.
3 – $commentaire = $_POST|'commentaire_commande'] ;
4 – $commentaire = htmlspecialchars ($commentaire) ;
5 – $requete = "update Commande set commentaire_commande =
6 –  '$commentaire'where id_commande = $_SESSION [IdCommande] ;
7 – mysqli_query ($requete) ;
```

1.3. En vous appuyant sur le schéma du réseau de Fermabio, expliquez quelles sont les configurations qui garantissent une disponibilité du site extranet.

D'après le schéma réseau de Fermabio, deux éléments contribuent à garantir la disponibilité du site extranet :

- la présence d'un cluster de pare-feu PfSense : en cas de panne d'un pare-feu, le second prend le relais, ainsi le site extranet est toujours accessible depuis l'extérieur (Internet) ;
- La présence de deux FAI (Free et SFR) : en cas de panne d'un FAI, le second peut prendre le relais. De plus ces deux liaisons offrent le même débit ce qui permet une bascule sans dégradation des performances.

1.4. Indiquez, en justifiant, si le résultat du test n° 2 révèle un problème de sécurité.

Oui, il y a bien un problème de sécurité. En effet, la somme de contrôle calculée sur le fichier de configuration du serveur Web après l'attaque est différente de celle d'origine calculée avant l'attaque. L'intégrité de ce fichier de configuration est donc remise en cause.
L'attaquant peut avoir modifié la configuration de ce fichier pour des raisons malveillantes.

2 Améliorer la traçabilité des évènements informatiques de Fermabio, p. 182

2.1. Expliquez le problème posé par la configuration d'enregistrement des journaux systèmes de Fermabio.

D'après le document 4, Fermabio ne dispose pas d'une procédure de collecte des journaux systèmes efficace et en conformité avec les recommandations de l'ANSSI. En effet :

- l'horodatage du serveur de collecte des traces n'est pas correct car il indique un fuseau horaire américain : les évènements collectés n'indiquent pas la bonne heure et sont donc peu exploitables ;
- la collecte se fait en temps différé alors que l'ANSSI recommande une collecte en temps réel (voir Fiche savoirs technologiques 11, p. 173) ;
- les journaux systèmes ne sont pas centralisés ce qui peut entraîner des incohérences (voir Fiche savoirs technologiques 11, p. 173) ;
- le protocole utilisé pour le transfert des journaux systèmes est http. Or ce protocole n'est pas sécurisé (voir Fiche savoirs technologiques 10, p. 153).

2.2. Listez les modifications à apporter pour disposer d'un système de traçabilité conforme aux recommandations d'usage.

Les modifications à apporter sont les suivantes :

- mettre le cluster de pare-feu à l'heure avec le bon fuseau horaire ;
- collecter les journaux systèmes en temps réel et centraliser ces journaux via l'utilisation d'un serveur de *logs* du type SYSLOG (voir document 2, p. 163) ;
- chiffrer la procédure de transfert des journaux systèmes vers le serveur de *logs* en utilisant le protocole HTTPS (voir Fiche savoirs technologiques 10, p. 153).

Entraînement à l'épreuve E6

Dossier A Déployer les moyens appropriés de preuves électroniques

1 Analyser des risques sur les traitements des données à caractère personnel, p. 187

1.1. Identifiez deux scénarios probables, en dehors de celui déjà proposé en exemple dans le document A2, mettant en jeu la protection des données à caractère personnel collectées pendant le vol de reconnaissance.

- **Document A.2 : Risques identifiés sur les données à caractère personnel**

Scénario 1	Perte de la carte SSD de la part du pilote réalisant le vol de reconnaissance. La perte de la carte est courante avec des conséquences importantes du fait de la perte de données.
Scénario 2	Consultation des données par une personne malveillante sur le poste de travail du pilote. Cela nécessite d'avoir accès à la session du pilote sur son poste de travail. Les conséquences sont importantes si les données sont modifiées ou supprimées.
Scénario 3	Écoute et modification de données pendant le transfert depuis le poste de travail du pilote vers l'espace de stockage hébergé chez VID&O afin de déstabiliser la position concurrentielle de l'entreprise. L'action nécessite des compétences techniques.

1.2. Analysez la vraisemblance de chaque scénario et la gravité des risques sur les traitements des données à caractère personnel.

- **Document A.3 : Niveaux de vraisemblance d'une menace**

Source de menace	Type de menace	Bien support	Niveau de vraisemblance	Critères de sécurité mis en jeu		
				C	D	I
Scénario 1	Menace non intentionnelle	Carte SSD	3 - Important (la perte d'une carte SSD est très courante du fait de sa petite taille)		X (La perte de la carte rend indisponible les données qu'elle contient)	
Scénario 2	Espionnage	Poste de travail	2 - Limité (si la session du pilote est accessible, c'est par simple manque de vigilance de sa part)	X (Les données deviennent accessibles grâce aux identifiants de connexion du pilote)		

Source de menace	Type de menace	Bien support	Niveau de vraisemblance	Critères de sécurité mis en jeu	Source de menace	Type de menace
				C	D	I
Scénario 3	Déstabilisation	Liaison réseau	3- Important (faille facilement exploitable par une personne malveillante)			X (Les données peuvent être modifiées pendant leur transfert)

C : Confidentialité ; D : Disponibilité ; I : Intégrité.
Mesure de la vraisemblance : 1 - Négligeable ; 2 - Limité ; 3 - Important ; 4 - Maximal.

- **Document A.4 : Niveau de gravité d'un risque**

Scénario 1	Perte de la carte SSD	Niveau de gravité : Important Les données confidentielles peuvent être utilisées par une personne non habilitée.
Scénario 2	Consultation de données sur le poste de travail du pilote	Niveau de gravité : Important Les données confidentielles peuvent être utilisées par une personne non habilitée.
Scénario 3	Écoute et modification de données pendant le transfert vers les serveurs de VID&O.	Niveau de gravité : Maximal Les données confidentielles peuvent être utilisées dans l'objectif de modifier la position concurrentielle de l'entreprise pouvant engendrer des pertes d'image et financière importantes.

Mesure de la gravité : 1 - Négligeable ; 2 - Limité ; 3 - Important ; 4 – Maximal.

1.3. Proposez une solution technique pour chaque scénario de menaces permettant de renforcer la protection des données à caractère personnel.

- **Scénario 1 : Perte de la carte SSD**

Le stockage des données peut être réalisé sur deux supports différents (deux cartes SSD) avec un cryptage des données dès l'enregistrement. Pour éviter de transporter la carte SSD jusqu'au lieu de travail du pilote, celui-ci pourrait disposer d'un poste de travail mobile qu'il amènerait à l'endroit du vol de reconnaissance.

- **Scénario 2 : Consultation de données sur le poste de travail du pilote**

Un rappel à la vigilance est un principe de base mais il faut surtout revoir la politique de mots de passe. Le mot de passe doit être fort et changé régulièrement par le pilote.

- **Scénario 3 : Écoute et modification de données pendant le transfert vers les serveurs de VID&O**

L'utilisation d'une encapsulation dans un protocole de transport sécurisé comme TLS doit être privilégiée entre le poste de travail pilote et les serveurs de VID&O.

2 Vérification de la conformité avec la législation du traitement des données personnelles, p. 187

2.1. Retrouvez, parmi les engagements du sous-traitant, ceux qui peuvent contribuer à renforcer la protection des données à caractère personnel.

- **Engagement 1 :** une réutilisation commerciale ou un transfert vers des organisations tierces sont exclus, ce qui limite les risques de diffusions de données à caractère personnel.
- **Engagement 3 :** en situation de violation des données, le client reçoit une notification précisant la nature de l'incident, les conséquences prévisibles et les mesures prises par VID&O. Cela permet au client de VID&O de préparer une réponse à la violation de données.

2.2. Identifiez l'acteur responsable de la publication d'images privées sur le site de l'exploitant.

La société DRONE-SECURITE est responsable des prises de vues aériennes réalisées sur l'exploitation agricole. Elle n'a pas respecté la vie privée et le droit à l'image du voisin de l'exploitant.

L'exploitant agricole est également responsable du respect du droit à l'image de son voisin. Il ne doit pas diffuser les captations de la propriété privée de son voisin sur son site sans autorisation.

Extrait des textes réglementaires pour information

- **Respecter la vie privée des autres**

Il est interdit de survoler et de filmer un espace privé (maison, jardin, etc.) et toute personne s'y trouvant sans l'autorisation du propriétaire et des personnes concernées.
Toute atteinte à la vie privée d'autrui (son intimité et son image) est punie d'une peine d'un an d'emprisonnement et de 45 000 € d'amende (article L226-1 du Code pénal).

- **Respecter le droit à l'image**

En vertu de la loi du 6 janvier 1978 modifiée dite « Informatique et Libertés », il est interdit de :

- diffuser des images permettant d'identifier des personnes (visages, plaques d'immatriculation, etc.) sans l'accord de celles-ci ;
- réutiliser des images ayant trait à la vie privée à des fins commerciales ou professionnelles.

2.3. Proposez une solution technique permettant une mise en conformité de la protection des données à caractère personnel.

Un rappel à la loi doit déjà être fait auprès des pilotes de drones.
De plus, les captations pourraient être d'abord cryptées, puis retravaillées – soit par DRONE-SÉCURITÉ, soit par son sous-traitant VID&O – pour assurer le respect de la loi sur la protection des données à caractère personnel.
En tout état de cause aucune image permettant d'identifier clairement la propriété du voisin ne doit être communiquée à l'exploitant agricole.

Dossier B L'impact de la nouvelle activité sur l'identité numérique de DRONE-SÉCURITÉ

1 Protection de l'identité numérique de l'organisation suite à une attaque par usurpation d'identité, p. 188

1.1. Repérez les éléments, dans le courriel reçu par l'exploitant agricole, permettant de reconnaître une opération d'hameçonnage.

L'hameçonnage (*phishing*) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels en usurpant l'identité d'une entreprise. Dans le document, les éléments permettant de reconnaître une tentative d'hameçonnage sont :

- un courriel impersonnel (*Cher(e) client(e)*) ;
- les fautes d'orthographe et les erreurs de syntaxe (a facilit**er**, recours **a** ses différents services, DRONE-SECURITE **à** l'honneur, supports propos**e**s) ;
- une source de confiance : ici, l'équipe commerciale de Drone-Sécurité ;
- l'invitation à se rendre sur une page de formulaire sur laquelle seront demandées et récupérées des données personnelles (identifiant, mot de passe et numéro client) ;
- l'adresse URL du lien et l'adresse mail de l'expéditeur sont maquillées afin de paraître authentiques (drone**s**-securite@services-clients.fr, http://www.drone**s**-securité.fr).

1.2. Identifiez les risques pour DRONE-SECURITE de la multiplication des avis négatifs publiés sur les réseaux sociaux en rapport à cette cyberattaque.

Une attaque d'hameçonnage réussie peut avoir des risques :

- sur l'e-réputation de la marque : avec la colère des consommateurs suite aux nombreux avis négatifs sur Twitter (bad buzz) ;
- économique : avec des pertes financières directes dues au ralentissement de l'activité de l'entreprise, aux coûts générés par des mesures de protection des données ou des actions de communication pour restaurer l'e-réputation de l'entreprise ;
- juridique : par les démarches pour la protection de la propriété intellectuelle de la marque.

1.3. Proposez une solution technique qui permettrait de sécuriser les échanges entre la société et ses clients.

Selon la CNIL, la messagerie électronique ne constitue pas un moyen de communication sûr pour transmettre des données personnelles, sans mesures complémentaires. Lors d'un envoi, des précautions élémentaires sont à prendre :

- chiffrer les pièces sensibles en utilisant des fonctions cryptographiques ;
- utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers ;
- assurer la confidentialité des secrets (clé de chiffrement, mot de passe, etc.) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par e-mail et communication du mot de passe par téléphone ou SMS).

2 Déploiement de moyens appropriés de preuves électroniques liées à l'usurpation d'identité, p. 188

2.1. Repérez les éléments dans l'URL du lien communiqué qui permettent d'identifier une attaque par typosquattage.

Le typosquattage (*typosquatting*) est une variante de l'attaque par hameçonnage qui mise sur les fautes de frappe ou d'orthographe des utilisateurs lorsqu'ils renseignent l'URL. Concrètement, les pirates réservent des noms de domaine avec des fautes d'orthographe dans l'URL. Dans le site officiel, drone-securite.fr ne prend pas de « s » à la différence du faux site drone**s**-securite.fr

2.2. Identifiez les risques juridiques encourus pour DRONE-SECURITE par le typosquattage de son site et le recueil de données personnelles de ses clients.

L'organisation est juridiquement responsable de la mise en conformité avec le RGPD en matière de protection des données personnelles. En cas d'acte malveillant à l'encontre de son système d'information, DRONE-SECURITE doit apporter les preuves prouvant qu'elle a bien respecté ses obligations légales. Sinon, les utilisateurs disposent de deux recours contre DRONE-SÉCURITÉ :

- un recours civil : demande de dommages et intérêts pour réparer le préjudice,
- un recours pénal : demande de sanctions en cas de vol de données et défaut du respect des précautions utiles pour préserver la sécurité des données.

2.3. Rédigez une note avec vos recommandations sur les moyens de défense face à une attaque de ce type.

Pour protéger DRONE-SÉCURITÉ, il est possible d'agir :

- en amont, par la protection des éléments d'identification numérique, comme le nom de domaine. La réservation du nom de domaine suit la règle du « premier arrivé, premier servi ». Il est donc possible de racheter des noms de domaine approchants le site original de DRONE-SÉCURITÉ ;
- en aval, par le recours d'une voie extrajudiciaire nommée UDRP (*Uniform domain name dispute resolution policy*) en établissant le mauvais usage du nom de domaine par le pirate sauf pour les extensions en. fr et. re qui passent par la procédure PAR ;
- à tout instant, sur la base de l'article L.45-2 du Code des postes et des communications, si un intérêt légitime peut être prouvé sur un nom de domaine afin d'éviter qu'une personne soit susceptible de porter atteinte à des droits fondamentaux de propriété intellectuelle ou de la personnalité de DRONE-SÉCURITÉ.

Dossier C La sécurisation de l'usage des drones par les exploitants

1 Création des éléments d'authentification, p. 189

1.1. Expliquez pourquoi le formulaire de création des identifiants de connexion permet une authentification sécurisée.

Le formulaire de création de mots de passe impose des contraintes pour obtenir un mot de passe fort (robuste). Ainsi, par l'utilisation des expressions régulières ou regex (pour *regular expression*), l'utilisateur doit obligatoirement créer un mot de passe qui comporte des caractères alphanumériques, des caractères spéciaux, des majuscules et minuscules.
La longueur du mot de passe est également imposée (huit caractères minimum).
Ainsi le formulaire permet de créer un mot de passe qui respecte les préconisations de l'ANSSI. Seule l'utilisation d'une *passphrase* n'est pas imposée.
La deuxième partie du document montre que le mot de passe est testé pour vérifier qu'il n'est pas similaire à un mot de passe courant présent dans le dictionnaire « dictionnaire.txt », limitant les risques d'attaque par dictionnaires.

1.2. Précisez l'objectif de la procédure d'authentification décrite. Justifiez votre réponse en spécifiant le type d'authentification utilisé.

La procédure indique que, lors du processus d'authentification, l'utilisateur saisit d'abord son identifiant et son mot de passe. Cette saisie permet de générer l'envoi d'un code aléatoire unique transmis par SMS sur le smartphone et de rediriger l'utilisateur vers une deuxième page d'authentification sur laquelle il saisit le code transmis. Il s'agit d'une authentification à double facteur : quelque chose que je sais (mes identifiants) et quelque chose que je possède (mot de passe temporaire).

1.3. Indiquez si la procédure d'initialisation des drones chez DRONE-SÉCURITÉ permet d'éviter les failles de sécurité décrites dans l'étude.

La procédure permet de pallier une première faille de sécurité récurrente chez les IoT, à savoir l'utilisation d'éléments d'authentification préconfigurés, simples et courants (000).
En effet, l'utilisateur doit spécifier les éléments d'authentification présents sur la carte attachée au drone, donc unique et spécifique à chaque utilisateur. De plus, ces éléments peuvent être modifiés ensuite.
Cependant, il reste une faille de sécurité en rapport avec l'appareillage en WIFI ou en Bluetooth, car celui-ci est automatique sans la spécification d'une clé. Il serait judicieux de permettre la personnalisation d'un mot de passe pour l'appareillage et caché le SSID (individuel et fourni également sur la carte avec les éléments d'authentification).

2 Gestion des accès aux données, p. 189

2.1. Montrez comment la configuration des partages permet de contrôler l'accès aux données.

Le document 5 montre que le partage effectué sur les dossiers de stockage est personnalisé pour chaque agriculteur (son nom) et que les autorisations d'accès sont uniquement accordées à l'agriculteur concerné. « Tout le monde » et « utilisateur authentifié » ne sont plus activés.
Il en est de même pour les accréditations sur les fichiers : seul l'utilisateur concerné dispose de l'ensemble des ACL : lecture, modification, suppression, etc.

2.2. Précisez l'intérêt de séparer (dans un autre VLAN) le serveur de fichiers des autres serveurs.

La segmentation logique apportée à l'infrastructure physique de DRONE-SECURITE permet de cloisonner (compartimenter) les différents hôtes. Ainsi des contrôles réglementés peuvent être instaurés pour gérer la communication entre chaque hôte. En ne donnant accès qu'au VLAN du serveur de fichier, les utilisateurs ne pourront pas accéder aux autres serveurs ni à d'autres ressources du réseau local. L'objectif est de regrouper un ensemble d'hôtes de façon logique et indépendante (ici, les connexions VPN des différents agriculteurs).
Cela permet de créer des domaines de diffusion gérés par les commutateurs indépendamment de leur emplacement géographique. On imagine que des ACL seront configurées sur le routeur, interdisant la communication entre le réseau du serveur de fichiers et les autres sous-réseaux IP.

Dossier D La garantie de la disponibilité et de l'intégrité des services et des données

1 Sécurisation de la page d'authentification de GéoMap, p. 190

1.1. Précisez pourquoi le développement de la page d'authentification de GéoMap doit faire l'objet de toutes les attentions.

N'importe qui peut accéder au portail d'authentification de GéoMap via Internet et essayer de se connecter. Un pirate peut alors tenter de compromettre le système. Il est donc très important que cette page fasse l'objet d'un développement sécurisé.

1.2. Expliquez en quoi la première version du code source de la page d'authentification de GéoMap n'est pas sécurisée.

D'après le document 2, la première version du code de la page d'authentification, injecte les valeurs saisies par l'utilisateur (login et mot de passe) directement dans la requête SQL, sans effectuer de vérification de sécurité. En effet, la méthode *checkAuth* n'effectue pas ce type de vérification et cette méthode est appelée juste après la récupération des valeurs saisies. Il y a donc une carence de sécurité.

1.3. En vous appuyant sur les nouvelles méthodes développées par SIO-INFO, complétez le code source de la page d'authentification de GéoMap afin d'obtenir un codage sécurisé.

Il faut compléter le document D.4. Les ajouts de code à effectuer sont en gras.

```
1 InputAuthenticationHelper oneAuth = new InputAuthenticationHelper () ;
2 StringBuilder errMsg = new StringBuilder () ;
3 boolean SaisieSecurise = false ;
4 //On suppose que les variables loginSaisi et passwordSaisi contiennent les identifiants
5 // (login et mot de passe) saisis depuis le formulaire d'authentification.
6 // Test de la sécurité des identifiants saisis à compléter ici (question 3).
7 //Vérifications de sécurité
8 if ((oneAuth. isValidInput (loginSaisi) && oneAuth. isValidInput (passwordSaisi))
9  {
10    if ((oneAuth. isValidLength (loginSaisi) && oneAuth. isValidLength (passwordSaisi))
11    {
12              SaisieSecurise = true ;
13 }
14 }
15 if (SaisieSecurise){
16 //Vérification de l'identité via une requête SQL.
17 if (oneAuth. checkAuth (loginSaisi, passwordSaisi) {
18              //Succès d'authentification, accès au compte privé de l'utilisateur…
19 }
20 else {
21              errMsg. append ("Accès refusé, mauvais login et/ou mot de passe.\n") ; }
```



```
22 }
23 else {
24 errMsg. append ("Saisie non sécurisée.\n") ; }
```

2 Gestion des traces de tentatives d'authentification sur GéoMap, p. 190

2.1. Quel peut être l'intérêt de tracer les tentatives d'authentification ?

Tracer les tentatives d'authentification permet de repérer des tentatives de force brute sur des comptes utilisateurs. Un attaquant peut essayer plusieurs mots de passe de manière manuelle ou automatique via un outil de force brute afin de compromettre un compte.
Lorsque l'administrateur repère des tentatives d'echecs répétés, il peut prendre des mesures de protection (système de prévention d'intrusion IPS pour bannir l'adresse IP à l'origine de ces tentatives, par exemple).

2.2. Modifiez le code source de la page d'authentification de GéoMap afin d'appliquer la politique d'enregistrement des traces recommandée par SIO-INFO.

Il faut modifier le document D.4. Les ajouts de code à effectuer sont en gras. Seule la portion de code nécessaire est reprise dans cette correction. L'ancienne ligne 7 devient donc la ligne 15 car il y a du code à ajouter.

```
7 private static final String TAG = "GEOMAP";
8 //Récupération de la date du jour.
9 Date date = Calendar. getInstance (). getTime () ;
10 DateFormat dateFormat = new SimpleDateFormat ("dd-mm-yyyy hh : mm : ss") ;
11 String recupDate = dateFormat. format (date) ;
12 //Récupération de l'adresse IP de la connexion.
13 String recupIP = request.getHeader ("X- FORWARDED-FOR") ;
14 if (recupIP == null) { recupIP = request.getRemoteAddr () ; }
15 if (SaisieSecurise){
16 //Vérification de l'identité via une requête SQL.
17 if (oneAuth. checkAuth (loginSaisi, passwordSaisi) {
18       //Succès d'authentification, accès au compte privé de l'utilisateur…
19       Log. i (TAG, "Saisie utilisateur"+ loginSaisi + "de"+ recupIp + "à"+ recupDate + "

20                effectuée avec succès") ;
21 }
22 else {
23       errMsg. append ("Accès refusé, mauvais login et/ou mot de passe.\n") ;
24       Log. w (TAG, "Echec d'authentification utilisateur"+ loginSaisi +
25                      "de"+ recupIp + "à"+ recupDate) ;
26 }
27 }
28 else {
29       errMsg. append ("Saisie non sécurisée.\n") ;
```

```
30 Log. e (TAG, "Saisie utilisateur"+ loginSaisi + "de"+ recupIp + "à"+ recupDate + " non
31         conforme à la politique de sécurité") ;
32 }
```