



CYBERÉCURITÉ

des services informatiques



Sous la direction de François Saillard et David Balny
Patrice Dignan, Jérôme Parra, Jean-Pierre Souvarine



Flashez
moi !



DELAGRAVE

Pour l'enseignant

<http://www>

SUR LE SITE COMPAGNON



Livre du professeur



Ressources complémentaires

CYBERSÉCURITÉ

des services informatiques

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

Bloc de compétences n°3 - Cybersécurité des services informatiques (1^{re} année)

COMPÉTENCES	SAVOIRS ASSOCIÉS
Protéger les données à caractère personnel <ul style="list-style-type: none"> Recenser les traitements sur les données à caractère personnel au sein de l'organisation Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel Sensibiliser les utilisateurs à la protection des données à caractère personnel 	Savoirs technologiques <p>Typologie des risques et leurs impacts.</p> <p>Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve.</p> <p>Sécurité et sûreté : périmètre respectif.</p> <p>Sécurité des terminaux utilisateurs et de leurs données : principes et outils.</p> <p>Authentification, privilèges et habilitations des utilisateurs : principes et techniques.</p> <p>Gestion des droits d'accès aux données : principes et techniques.</p> <p>Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction physique et logique.</p> <p>Protection et archivage des données : principes et techniques.</p> <p>Chiffrement, authentification et preuve : principes et techniques.</p> <p>Sécurité des applications Web : risques, menaces et protocoles.</p> <p>Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique.</p>
Préserver l'identité numérique de l'organisation <ul style="list-style-type: none"> Protéger l'identité numérique d'une organisation Déployer les moyens appropriés de preuve électronique 	
Sécuriser les équipements et les usages des utilisateurs <ul style="list-style-type: none"> Informier les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter Identifier les menaces et mettre en œuvre les défenses appropriées Gérer les accès et les privilèges appropriés Vérifier l'efficacité de la protection 	Savoirs économiques, juridiques et managériaux <p>Les données à caractère personnel : définition, réglementation, rôle de la CNIL.</p> <p>L'identité numérique de l'organisation : risques et protection juridique.</p> <p>Droit de la preuve électronique.</p> <p>La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique.</p> <p>Les risques des cyberattaques pour l'organisation : économique, juridique, atteinte à l'identité de l'entreprise.</p> <p>Obligations légales de notification en cas de faille de sécurité.</p> <p>Réglementation en matière de lutte contre la fraude informatique : infractions, sanctions.</p> <p>Les organisations de lutte contre la cybercriminalité.</p>
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques <ul style="list-style-type: none"> Caractériser les risques liés à l'utilisation malveillante d'un service informatique Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation Organiser la collecte et la conservation des preuves numériques Appliquer les procédures garantissant le respect des obligations légales 	

Édition : Sébastien Le Jean

Conception maquette : Anne-Danielle Naname

Conception couverture : Christophe Trottier

Mise en page : Ghislaine Geneslay, Jean-Jacques Galmiche

© Delagrave Éditions 2020 – 5 allée de la 2e D.B., 75015 Paris

www.editions-delagrave.fr

Retrouvez-nous sur 

ISBN : 9782206306988

Sommaire

THÈME
1

Protéger les données à caractère personnel



CHAPITRE 1 Identifier les risques liés aux données à caractère personnel 11

CHAPITRE 2 Appliquer et diffuser la réglementation liée aux données à caractère personnel 33

Évaluation 1 51

THÈME
3

Sécuriser les équipements et les usages des utilisateurs



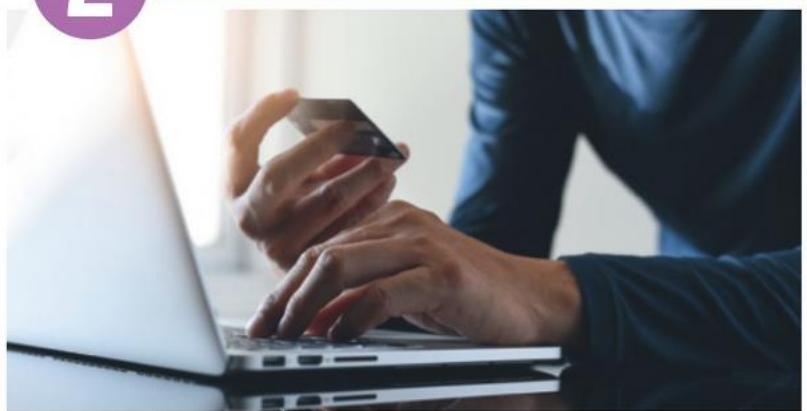
CHAPITRE 4 Informer les utilisateurs et mettre en œuvre les défenses appropriées 85

CHAPITRE 5 Sécuriser l'accès aux ressources et vérifier l'efficacité 107

Évaluation 3 131

THÈME
2

Préserver l'identité numérique de l'organisation



CHAPITRE 3 Préserver l'identité numérique de l'organisation 57

Évaluation 2 79

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 137

CHAPITRE 7 Archiver et protéger les données et les preuves numériques 161

Évaluation 4 181

Entraînement à l'épreuve E6 185

Les outils pour réussir

Fiches méthode

203

Lexique

221

Sommaire des fiches savoirs

Fiche savoirs technologiques

1	La typologie des risques et leurs impacts	23
2	Les principes de la sécurité	25
3	Sécurité et sûreté	26
4	La sécurité des terminaux utilisateurs et de leurs données	99
5	Les authentifications, privilèges et habilitations des utilisateurs	119
6	La gestion des droits d'accès aux données	121
7	La sécurité des communications numériques	123
8	La protection et l'archivage des données	149
9	Le chiffrement, l'authentification et la preuve	151
10	La sécurité des applications Web	153
11	Les plans de secours, la traçabilité et l'audit technique	173

Fiche savoirs CEJM appliquée

1	Les traitements sur les données à caractère personnel	28
2	Les données à caractère personnel : réglementation, rôle de la CNIL	45
3	L'identité numérique de l'organisation : risques et protection juridique	69
4	Le droit de la preuve électronique	71
5	Les risques des cyberattaques pour l'organisation	73
6	La sécurité des équipements personnels des utilisateurs et de leurs usages	101
7	Les obligations légales de notification en cas de failles de sécurité	125
8	La réglementation en matière de lutte contre la fraude informatique	155
9	Les organisations de lutte contre la cybercriminalité	175



Les activités numériques

En accès gratuit pour tous

Tout au long du manuel des liens ou codes à flasher vous donnent accès à des ressources numériques.

7 QCM autocorrectifs pour tester ses connaissances sur chaque chapitre.

DELAGRAVE

Chapitre 1 – Identifier les risques liés aux données à caractère personnel

Pour chaque proposition, choisir la (les) bonne(s) réponse(s).

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

1 sur 4



Retrouvez ce QCM
en version interactive
www.lienmini.fr/6988-105

Des vidéos pour découvrir les notions du programme et les entreprises citées en exemple.



VIDÉO

Immersion dans le métier de CentreCall

www.lienmini.fr/6988-1001

Les **machines virtuelles** pour les manipulations sur poste informatique

Comment accéder à ces activités ?

- Depuis une tablette ou un smartphone, en scannant le QR Code.
- Depuis un ordinateur, en saisissant le lien mini dans un navigateur.

Présentation du livre

Contexte 1

Protéger les données à caractère personnel

L'organisation cliente

Réalisé en 1998, l'entreprise CentreCall propose des centres d'appels implantés dans des bâtiments de bureaux : à Lille, Paris, Lyon, Reims et Strasbourg. Ses sites sociaux se situent à Rouen, dans les locaux de la Cnil.

Les centres d'appel sont des plateformes qui gèrent l'accès à l'éphonique ou des démarches d'information pour le compte d'entreprises clientes.

En confirmant l'externalisation de ces services à CentreCall, ces entreprises peuvent se concentrer sur leur cœur de métier.

Le prestataire informatique

La direction des systèmes d'information (DSI), installée dans les bâtiments du siège social de CentreCall, est dirigée par Mme Azri. Elle est responsable en trois pôles de compétences :

- le pôle Infrastructures et services a pour activité principale le paramétrage et la sécurisation des éléments d'interconnexion et des serveurs;

CentreCall a été évalué par la Cnil pour la protection des données à caractère personnel.

CHAPITRE
1

Identifier les risques liés aux données à caractère personnel

COMPÉTENCES

- Recenser les traitements sur les données à caractère personnel au sein de l'organisation
- Identifier les risques liés à la collecte, au traitement ou à la mise en œuvre des données à caractère personnel
- Typologie des risques et leurs impacts
- Principes de la sécurité : disponibilité, intégrité, confidentialité, privacé
- Sécurité et droit : prédroits respect
- Les traitements sur les données à caractère personnel

SAVOIRS ACQUISIS

- Décrire quelques risques pour la situation d'étude de marché.
- Sur cette même période, des incidents ont été causés à partir ou en direction de données dont certaines sont à caractère personnel.
- Ces incidents peuvent avoir des conséquences catastrophiques pour la réputation de CentreCall et engager des pertes financières importantes.
- Mme Azri a également décidé de renforcer les mesures de sécurité lors des processus d'étude de marché afin de mieux identifier les risques qui pèsent sur la protection des données à caractère personnel.

Situation professionnelle

Depuis quelques mois, CentreCall observe une forte croissance de la demande de ses clients pour la réalisation d'études de marché.

Sur cette même période, des incidents ont été causés à partir ou en direction de données dont certaines sont à caractère personnel.

Voir présentation générale, p. 9

CHAPITRE
1

Missions professionnelles

Recenser les traitements sur les données à caractère personnel

Le traitement des données à caractère personnel fait à la réalisation d'étude de marché doit être conforme avec les directives de la CNIL.

Mme Azri vous demande d'aider vos collègues à identifier les données à caractère personnel et à recenser les traitements réalisés.

Pour cette mission, vous devez prendre en compte les contraintes spécifiques en matière de traitement des données qui pèsent sur les centres d'appel de CentreCall.

Trajet à faire

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

Document 1 Fiche exercice CEINTURE 1

Après réception de l'accord oral de la personne interrogée, les opérateurs du centre d'appel peuvent arrêter la conversation téléphonique afin de ne pas communiquer d'informations dans la collectivité interrogée. Dans ce cas, les opérateurs précisent la finalité de l'enquête.

2. Ajustez la conformité de la situation décrite ci-dessous avec les directives de la CNIL.

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

Document 2 et 4

CentreCall décline mobiliser plusieurs canaux (par exemple : courriel, téléphone et SMS) pour sa collecte de données. L'application Complus SMS (document 4) est actuellement testée pour accompagner cette démarche. Certains incidents sont malheureusement déjà rencontrés.

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

Document 3 et 4

Voir fiche B15 SIO 5, p. 221

Des chapitres construits autour de **situations professionnelles** variées pour travailler en contexte.

Dossier documentaire

Document 1 Extrait des données recueillies lors d'une étude de marché

Le client final de CentreCall souhaite recueillir des données sur les attentes du marché de la publicité relatives aux réseaux sociaux. Voici un extrait du questionnaire.

Question 1 - Possédez-vous un smartphone ?
 OUI NON

Question 2 - Quels réseaux sociaux avez-vous l'habitude de fréquenter ?
 Plusieurs fois par jour Une fois par jour Une fois par semaine Pas du tout

Question 3 - À quelle fréquence utilisez-vous ce réseau ?
 Plusieurs fois par jour Une fois par jour Une fois par semaine Pas du tout

Question 4 - Pour vous, la publicité sur les réseaux sociaux :
 est intéressante vous aide à saisir des opportunités intéressantes vous laisse méfiant(e)

Bonpoint 1 Faut-il informer les clients de l'enregistrement des conversations téléphoniques ?

Chaque interlocuteur (particulier, client, etc.) doit être informé au moment de son appel :

- de son droit d'accès aux enregistrements.
- de l'objectif de l'enregistrement.
- des destinataires des données ou enregistrements (service de formation, service client, etc.).

Document 2 Tableau de recensement des opérations réalisées pour une étude de marché

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	à la personne	Prospect	Client et service interne de CentreCall

CHAPITRE 1 Identifier les risques liés aux données à caractère personnel

Des **missions professionnelles** prenant appui sur un dossier documentaire, sous forme d'étude de cas, pour se préparer à l'épreuve finale E6.

PHOTO : © PHOTODISC/GETTY IMAGES, © PHOTODISC/GETTY IMAGES, © PHOTODISC/GETTY IMAGES, © PHOTODISC/GETTY IMAGES

Travaux en laboratoire informatique

1 Recenser les traitements sur les données à caractère personnel au sein de l'organisation

La société Artemis souhaite bénéficier des services de CentreCall pour externaliser le processus de fidélisation de sa clientèle. Mme Azri, responsable des données chez CentreCall, profite de votre présence à la réalisation des missions à caractère personnel et leurs travaux doivent vous aider à faire le travail de ce dossier. Un dossier documentaire est à votre disposition pour vous aider dans votre mission.

1. Schématissez 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 traitées au processus de fidélisation.

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

Une déclaration des traitements réalisés sur des données à caractère personnel doit être effectuée auprès de la CNIL. Pour cela, un document numérique doit être complété par l'organisation.

4. À l'aide des documents 2 et 3, complétez le registre numérique des activités de traitement (2 et 5) du document numérique en tenant compte des réponses apportées aux questions précédentes pour le processus de fidélisation.

5. Rédigez numériquement des actes à compléter : www.cnil.fr/100818

Document 1 Extrait de l'entretien entre Mme Azri et la société Artemis

M. Friend : Bonjour Mme Azri. Je suis Paul Friend, directeur de la société Artemis. Afin de nous renseigner sur notre cœur de métier, nous souhaitons vous confier la clé pour réussir la fidélisation de nos clients. Pourriez-vous nous indiquer les éléments dont vous avez besoin pour cette phase en charge ?

M. Friend : Quelle est la confiance que vous portez à notre entreprise. Nous croyons à l'avenir de notre entreprise pour optimiser cette fidélisation. Nous croyons à l'avenir de notre entreprise pour optimiser cette fidélisation.

M. Friend : Nous disposons de toute notre essentielle.

1 Travaux en laboratoire informatique

1 Informations complémentaires

• Date de création de la fiche de registre : 15/05/2020

• Durée de conservation des données à caractère personnel : 3 ans

• Autres destinataires des données : Protection des services de base de données, par un passeur, sous-traitants, récepteurs, réceptrices des données et accès aux données par authentification.

Document 2 Obligations pour le registre des traitements

Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité. Lorsque de nouveaux traitements et d'opérations, il doit se faire connaître de tous les intervenants, soit les personnes et vous pourrez l'identifier précisément :

- « les parties prenantes (consommateurs, sous-traitants, responsables, etc.) qui interviennent dans le traitement des données ;
- « à qui sont cédées les données (ce qui sera en fait), qui accède aux données et à qui elles sont communiquées ;
- « combien de temps vous les conservez ;
- « comment elles sont sécurisées.

www.cnil.fr

Des **travaux en laboratoire informatique** dédiés aux 2 heures hebdomadaires sur poste informatique et pour se préparer à l'épreuve E5.

BTS SIO © DELAGRAVE, 2020. La photocopie non autorisée est un délit.

6

Présentation du manuel

Fiche savoirs technologiques 1

La typologie des risques et leurs impacts

I Définitions de vulnérabilité, menace et risque

Vulnérabilité	Menace	Risque
Un intérêt, une situation ou une habileté de l'organisation qui peut entraîner des dommages sur le SI	Une menace est une cause interne ou externe susceptible d'entraîner des dommages sur le SI	Un risque est la combinaison de la probabilité de l'explosion d'une vulnérabilité et/ou d'une menace. Le niveau d'un risque est évalué en fonction de la probabilité de l'apparition de la vulnérabilité et de la gravité de son apparition

Les objectifs de la sécurité informatique consistent à limiter les vulnérabilités et les risques.

II La typologie des risques informatiques

1. La méthode EBOS

EBOS Risk Manager (l'expression des besoins et identification des objectifs du risque) et EBOS Management of Risk (évaluation de la sécurité des systèmes d'information et retour au CNET). L'approche EBOS permet d'identifier et de hiérarchiser les différents risques dans un contexte clairement défini. Un risque est défini par l'ANSSI comme « un scénario qui combine un événement redouté et un ou plusieurs scénarios de menaces ». Un événement redouté désigne par exemple la possibilité d'atteindre des données avec des conséquences probables sur la vie privée des personnes concernées.

2. L'évaluation des risques

L'évaluation des impacts des risques informatiques est réalisée par le croisement de son niveau de vulnérabilité et de gravité.

Exemple de cartographie des risques :

La vulnérabilité reflète la probabilité ou la possibilité que l'un des modes opératoires de l'attaquant aboutisse à l'objectif visé. Elle dépend des vulnérabilités des supports face aux menaces et des capacités des sources de risque à les exploiter.

Fiche savoirs technologiques 1

La gravité évalue l'enjeu d'un événement redouté sur des « valeurs majeures », c'est-à-dire stratégiques pour l'organisation : informations confidentielles, processus métier, matériels, logiciels, etc.

Exemple de mesure de la gravité :

Valeur majeure	Événement redouté	Impact	Gravité
Facturation	Altération des informations sur les factures	• Impossibilité de facturer ou de payer • Perte de clients • Impact sur la réputation et les chiffres logiciels	G-très

III Les impacts des risques informatiques

L'ANSSI, au travers de sa méthode EBOS, identifie différentes catégories d'impacts.

Catégorie	Impact
Impacts sur les missions et les services de l'organisation	<ul style="list-style-type: none"> Impacts sur la sécurité ou sur la santé des personnes : conséquences sur l'entourage physique des personnes. Impacts matériels : dégâts matériels ou destruction de biens supports. Impacts sur l'environnement : conséquences écologiques à court ou long terme.
Impacts sur la personne	<ul style="list-style-type: none"> Impacts sur la capacité de développement ou de décision : conséquences sur la liberté de décision, de diriger, de mettre en œuvre la stratégie de l'organisation. Impacts sur le bien social interne : conséquences sur la qualité des liens sociaux au sein de l'organisation. Impacts sur le bien social externe : conséquences sur l'environnement et/ou culturel ; conséquences sur les communautés et/ou personnes accueillies par l'organisation sur le secteur, les cascades d'innovation, les références culturelles communes.
Impacts financiers	Consequences pécuniaires.
Impacts juridiques	Consequences liées à une non-conformité légale, réglementaire, normative ou contractuelle.
Impacts sur l'image et la confiance	Consequences sur l'image de l'organisation, la notoriété, la confiance des clients.

Des **fiches savoirs technologiques** et **CEJM appliquée** claires et synthétiques pour retenir l'essentiel.

Des applications variées, sur table ou en laboratoire informatique, pour vérifier ses acquis

1 Applications

2 Analyser un PIA

Extrait de la politique de protection de la confidentialité des données personnelles de Castorama

3 Cartographier le traitement des données à caractère personnel

4 Repérer l'utilisation des données à caractère personnel

5 Traitements et risques sur les données à caractère personnel

1 Applications

1 QCM

Retrouvez ce QCM en version interactive www.lienmini.fr/6988-105

2 QCM

Des QCM numériques et autocorrectifs

Retrouvez ce QCM en version interactive www.lienmini.fr/6988-105



4 évaluations
sur chacun des thèmes

1 entraînement
à l'examen synthétique

Des fiches méthodes
pour les travaux en laboratoire

Un lexique
avec tous les mots-clés

Crédits photographiques

© Adobe Stock

Vous utilisez un **Manuel connecté Delagrave**, qui propose des QR codes et/ou des liens hypertextes permettant d'accéder en ligne à des ressources numériques complémentaires.

Les éditions Delagrave font leurs meilleurs efforts pour sécuriser la consultation et l'utilisation des ressources en ligne qu'elles éditent, produisent ou hébergent, conformément aux règles d'usages d'Internet. Delagrave ne saurait être tenu responsable des interruptions de services dues aux caractéristiques et limites du réseau Internet, notamment dans le cas d'interruptions quelle qu'en soit la cause, des performances techniques et des temps de réponse pour consulter ou interroger les ressources proposées. L'accès aux ressources associées au Manuel connecté Delagrave est garanti pour une période maximum de deux ans, à compter de la date de parution de cet ouvrage indiquée en page 2 (copyright). Au terme de cette période, l'utilisateur du Manuel connecté Delagrave ne saurait exiger le maintien du service proposé.

Dans le cas où les QR codes et liens hypertextes permettent d'accéder à des sites Internet tiers, la responsabilité des éditions Delagrave n'est pas engagée, notamment quant à leur éventuel dysfonctionnement ou à leur indisponibilité d'accès.



Tous droits de traduction, d'adaptation et de reproduction par tous procédés, réservés pour tout pays.

Le Code de la propriété intellectuelle n'autorisant, aux termes des paragraphes 2 et 3 de l'article L. 122-5, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, sous réserve du nom de l'auteur et de la source, que « les analyses et les courtes citations justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information », toute représentation ou reproduction intégrale ou partielle, faite sans consentement de l'auteur ou de ses ayants droit, est illicite (art. L. 122-4). Toute représentation ou reproduction, par quelque procédé que ce soit, notamment par téléchargement ou sortie imprimante, constituera donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Contexte 1

Protéger les données à caractère personnel



L'organisation cliente

Fondée en 1991, l'entreprise CentreCall compte cinq centres d'appels implantés dans des grandes villes en France : Lille, Paris, Tours, Bordeaux et Toulouse. Son siège social se situe à Tours, dans des locaux de 500 m².

Les centres d'appel sont des plateformes qui réalisent l'accueil téléphonique ou des démarches de télémarketing pour le compte d'entreprises clientes.

En confiant l'externalisation de ces services à CentreCall, ces entreprises peuvent se concentrer sur leur cœur de métier.

VIDÉO

Immersion dans le métier de CentreCall



www.lienmini.fr/6988-1001

Le prestataire informatique

La direction des systèmes d'information (DSI), installée dans les bâtiments du siège social de CentreCall, est dirigée par M^{me} Azri. Elle est organisée en trois pôles de compétences :

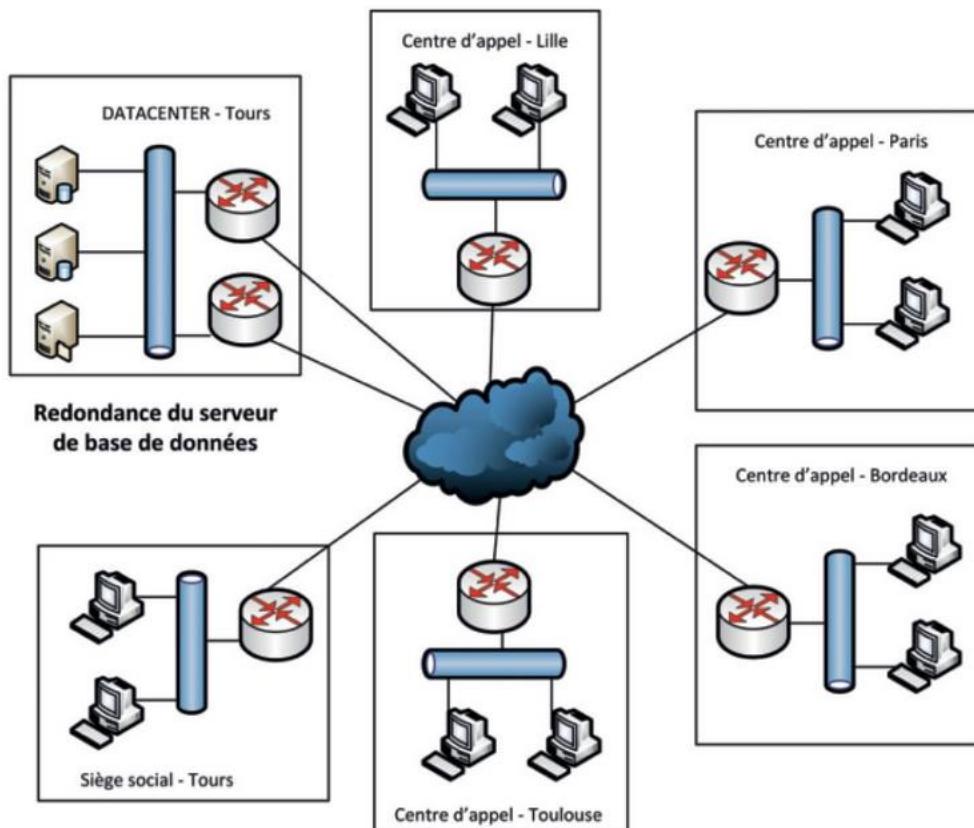
- le pôle Infrastructures et serveurs a pour activités principales le paramétrage et la sécurisation des éléments d'interconnexion et des serveurs ;

- le pôle Applications est dédié au développement d'applications spécifiques pour les besoins de CentreCall ;
- le pôle Données à caractère personnel et données sensibles a pour mission de veiller à l'identification des risques et au respect de la législation sur les données à caractères personnel.

Contexte 1

Description du SI de l'organisation

Schéma général du réseau de CentreCall



L'infrastructure informatique de CentreCall s'organise de la manière suivante :

- l'ensemble des sites est interconnecté par une liaison VPN (*Virtual Private Network*, en français « Réseau privé virtuel ») ;
- CentreCall assure une continuité des accès à ses serveurs *via* une redondance de ses éléments d'interconnexion ;
- la redondance des serveurs de base de données assure la continuité des accès aux données stockées, notamment aux données à caractère personnel.

Cahier des charges

Les activités de CentreCall conduisent M^{me} Azri à appliquer une politique rigoureuse en matière de protection des données à caractère personnel. Celle-ci doit répondre à quatre objectifs majeurs :

- le recensement des traitements des données à caractère personnel au sein de l'organisation, notamment lors des études de marché réalisées pour le compte des clients ;

- l'identification des risques liés aux traitements des données à caractère personnel durant le processus d'une étude de marché ;
- la vérification du respect de la législation en matière de traitement et de conservation des données à caractère personnel ;
- la sensibilisation des différents acteurs (opérateurs téléphoniques, managers, etc.) à la protection des données à caractère personnel.

Votre mission

Vous êtes accueilli(e) au sein du pôle Données à caractère personnel et données sensibles, situé dans les locaux de la DSI. Vous participez à différentes missions destinées à assurer la protection des données à caractère personnel collectées par CentreCall.

Identifier les risques liés aux données à caractère personnel

COMPÉTENCES

- Recenser les traitements sur les données à caractère personnel au sein de l'organisation
- Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel

SAVOIRS ASSOCIÉS

- Typologie des risques et leurs impacts
- Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve
- Sécurité et sûreté : périmètre respectif
- Les traitements sur les données à caractère personnel

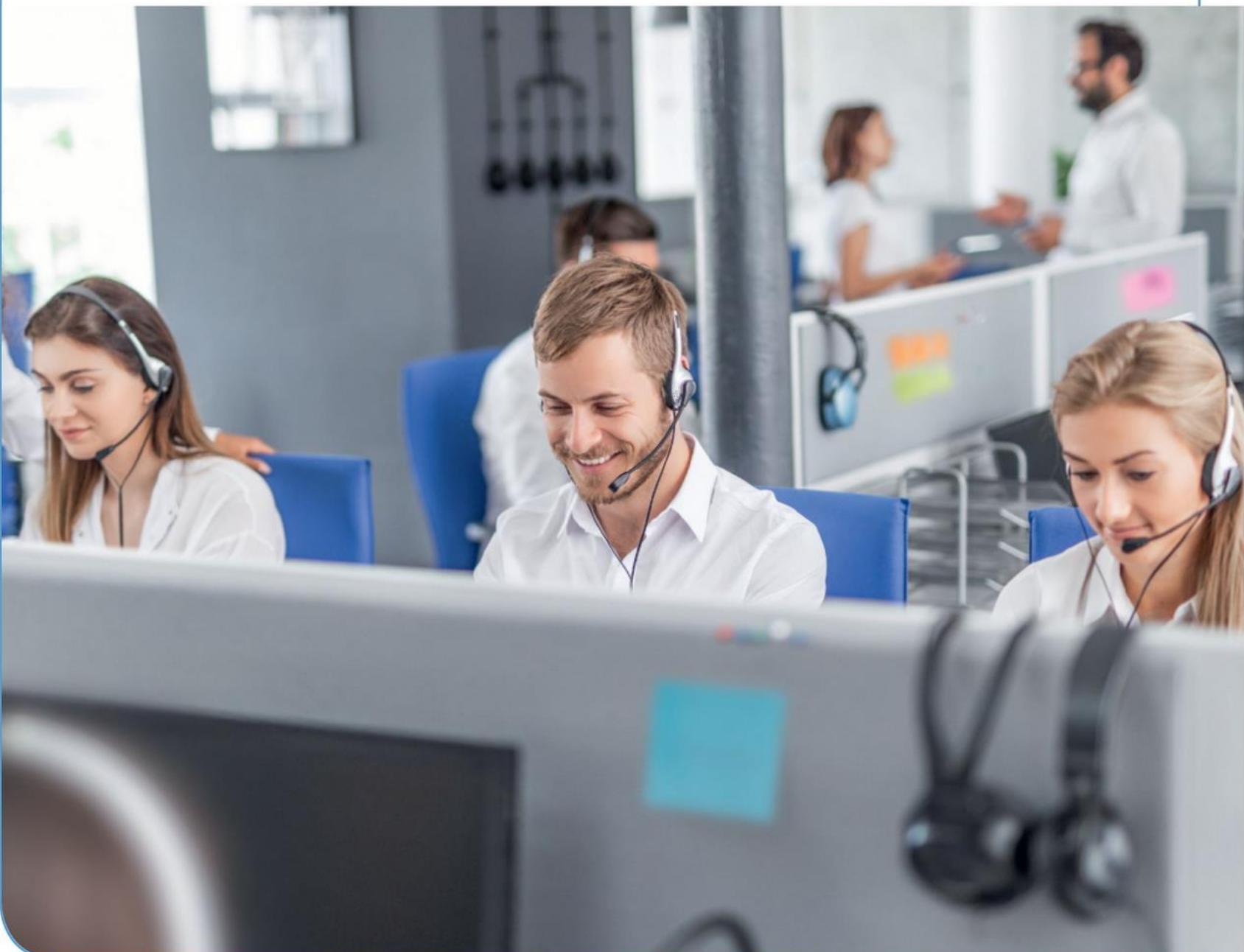
Situation professionnelle

Depuis quelques mois, CentreCall observe une forte croissance de la demande de ses clients pour la réalisation d'études de marché.

Sur cette même période, des incidents ont été constatés : perte ou divulgation de données dont certaines sont à caractère personnel.

Ces incidents peuvent avoir des conséquences catastrophiques pour la réputation de CentreCall et engendrer des pertes financières importantes.

M^{me} Azri vous demande de recenser les traitements réalisés lors du processus d'étude de marché afin de mieux identifier les **risques** qui pèsent sur la protection des données à caractère personnel.



➤ Voir présentation générale, p. 9

Missions professionnelles

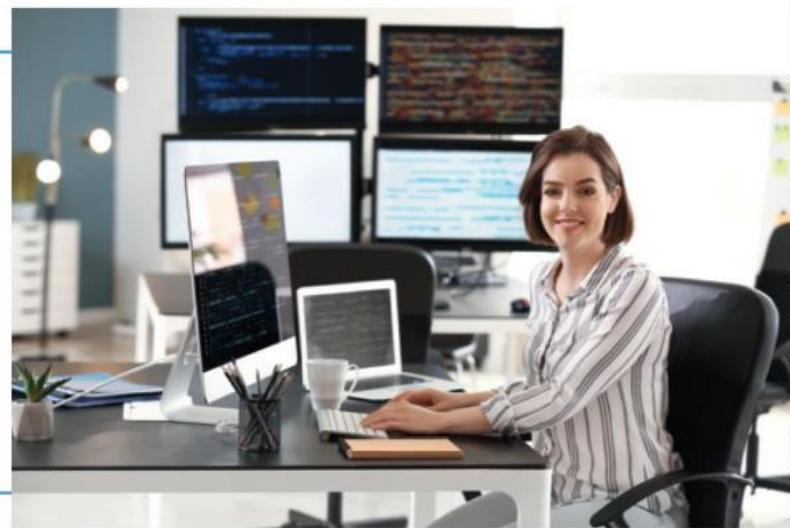
1

Recenser les traitements sur les données à caractère personnel

Le traitement des données à caractère personnel liées à la réalisation d'études de marché doit être conforme avec les directives de la **CNIL**.

M^{me} Azri vous demande d'aider vos collègues à identifier les données à caractère personnel et à recenser les traitements réalisés.

Pour cette mission, vous devez prendre en compte les contraintes spécifiques en matière de traitement des données qui pèsent sur les centres d'appel de CentreCall.



Travail à faire

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

- Fiche savoirs CEJMA 1
- Document 1

Après réception de l'accord oral de la personne interrogée, les opérateurs du centre d'appel peuvent enregistrer la conversation téléphonique afin de ne pas commettre d'erreurs dans la collecte des informations. Dans ce cas, les opérateurs précisent la finalité de l'enregistrement.

- Analysez la conformité de la situation décrite ci-dessus avec les directives de la **CNIL**.

- Document 2

Un de vos collègues de l'équipe informatique a schématisé le processus de gestion des appels téléphoniques pour la réalisation d'une étude de marché. Il a également réalisé un tableau permettant de lister les opérations effectuées sur les données à caractère personnel tout au long de ce processus.

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

- Documents 3 et 4

CentreCall désire mobiliser plusieurs canaux (par exemple : courriel, téléphone et SMS) pour sa collecte de données. L'application ComPlus SMS (document 6) est actuellement testée pour accompagner cette démarche. Certains incidents sont malheureusement déjà remontés.

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

- Documents 5, 6 et 7

Dossier documentaire

Document 1 Extrait des données recueillies lors d'une étude de marché

Le client Osiris de CentreCall souhaite recueillir des données sur les attentes du marché de la publicité relatives aux réseaux sociaux. Voici un extrait du questionnaire.

Nom : DESMARC
Prénom : CORINNE
Adresse complète : 2, place de l'Église – 37100 Tours
Courriel : desmarc.corinne@orange.fr

Question 1 - Possédez-vous un smartphone ?

OUI NON

Question 2 - Quels réseaux sociaux avez-vous l'habitude de fréquenter ?

Réponse : Facebook

Question 3 - À quelle fréquence utilisez-vous ce réseau ?

Plusieurs fois par jour Une fois par jour
 Une fois par semaine Plus rarement

Question 4 - Pour vous, la publicité sur les réseaux sociaux :

est intrusive.
 vous aide à saisir des opportunités intéressantes.
 vous laisse indifférent(e).

Document 2 Faut-il informer les clients de l'enregistrement des conversations téléphoniques ?

Chaque interlocuteur (particulier, client, etc.) doit être informé au moment de son appel :

- de l'objectif de l'opération ;
- des destinataires des écoutes ou enregistrements (service de formation, service client, etc.) ;

- de son droit d'opposition ;
- de son droit d'accès aux enregistrements.

Cette information peut être réalisée par la diffusion d'un message en début d'appel ou par une mention particulière dans les contrats ou documents d'information.

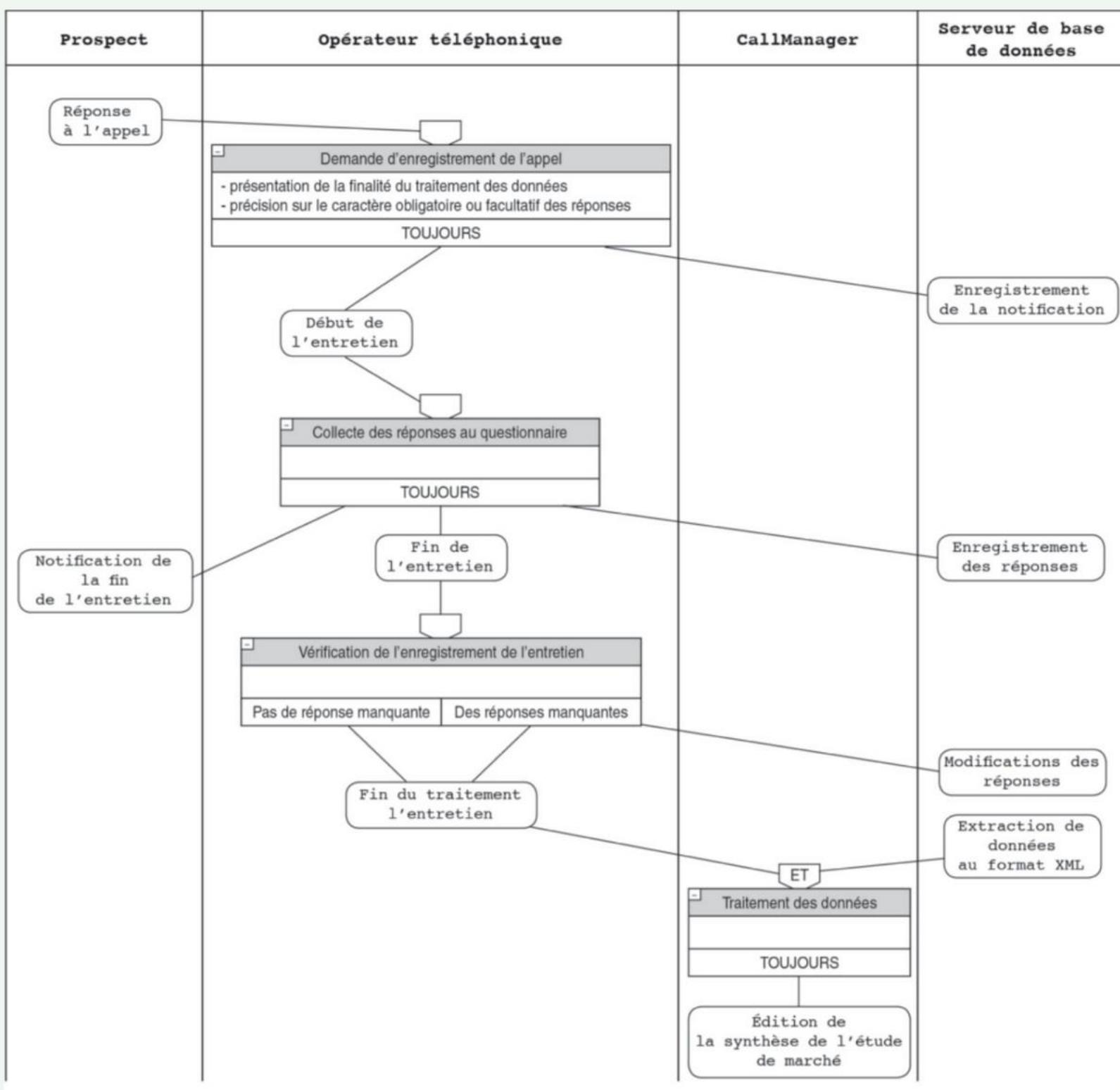
www.cnil.fr

Document 3 Tableau de recensement des opérations réalisées pour une étude de marché

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

Missions professionnelles

Document 4 Processus de réalisation d'une étude de marché chez CentreCall



Exemple de lecture d'une opération : la demande d'autorisation d'enregistrement d'un appel précède toujours l'enregistrement de l'acceptation de la personne interrogée et le début de l'entretien.

Document 5 CentreCall, un centre d'appel multicanal

L'appareillage des clients et la facilité d'accès à certaines informations via Internet oblige CentreCall à une transformation digitale. Le client peut établir le contact par courriel, puis par un appel téléphonique pour enfin suivre l'évolution de sa demande sur une application mobile.

CentreCall doit accompagner ce changement en adoptant le multicanal : les plateformes des centres d'appels sont désormais capables de gérer les demandes en provenance de plusieurs canaux (site internet, courriel, SMS, appel vidéo, etc.).

Document 6 Spécificités techniques de l'application ComPlus

L'application ComPlus a été développée spécifiquement pour CentreCall.

Le rôle de l'application est de collecter et de traiter des données issues du processus d'étude de marché collectées via différents canaux : courriel, SMS, appel téléphonique ou vidéo, formulaire sur le site Internet, application mobile fournie par la société.

ComPlus permet d'édition des synthèses d'études de marchés pour les clients et de bénéficier de rapports d'activités pour les *Call managers*.

La variété des solutions techniques entraîne une utilisation de différents formats de données.

Par exemple :

- les données collectées grâce au formulaire du site Internet de CentreCall peuvent être inserées directement dans la **base de données** de l'application ComPlus ;

- les données reçues par courriel, via l'utilisation d'un document au format PDF, sont traitées automatiquement par l'application ComPlus et enregistrées au format CSV avant d'être insérées dans la base de données ;
- les données collectées via l'application mobile sont transférées au format JSON (format proche du XML) puis traitées par la solution ComPlus avant une insertion dans la base ;
- d'autres données sont insérées directement dans la base de données par les opérateurs, car la source d'information n'est pas traitable automatiquement par l'application ComPlus (par exemple les enquêtes par téléphone ou visioconférences).

Document 7 Tickets d'incidents suite à l'utilisation de l'application ComPlus

L'application ComPlus est actuellement testée par quelques opérateurs téléphoniques et les *Call managers*. L'objectif est de repérer les incidents et apporter d'éventuels **correctifs**.

Deux tickets d'incidents sont déjà rédigés :

Ticket n° 1

Date : 20/05/202N

Origine : David Blanc (technicien informatique)

Objet : Bugs liés au typage de données

Message :

Bonjour,

J'ai constaté que le type « date » utilisé dans les données recueillies via les fichiers JSON est différent de celui prévu dans la base de données.

La conséquence est une inversion pour certaines dates entre le mois et le jour, ou encore la non prise en compte de certaines dates.

Ticket n° 2

Date : 14/06/202N

Origine : Christophe Vicq (*Call manager*)

Objet : Problème d'**intégrité** des données

Message :

Bonjour,

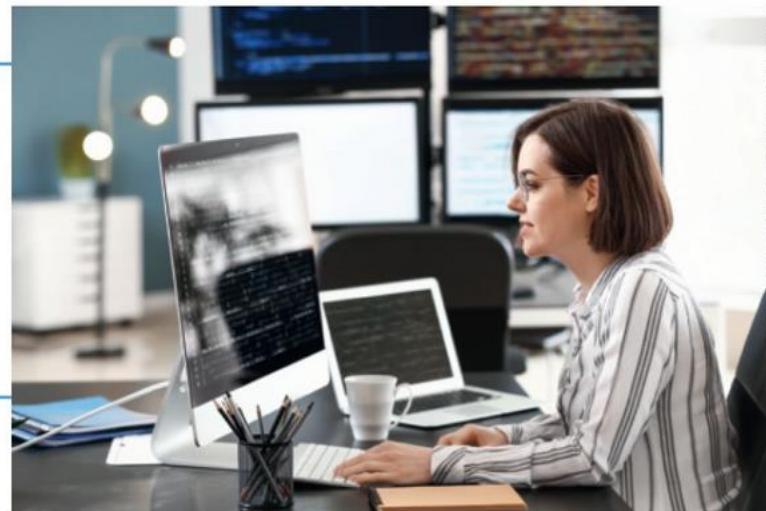
Je constate que l'utilisation de ComPlus n'a pas supprimé des problèmes d'incohérence entre des informations enregistrées lors d'entretiens téléphoniques et les données insérées dans la base.

Missions professionnelles

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

Mme Azri souhaite maintenant identifier les risques liés au traitement des données à caractère personnel dans le cadre du processus d'études de marché.

Pour réaliser ce travail, vous devez prendre appui sur la méthode PIA (*Privacy Impact Assessment*, en français « analyse d'impact relative à la protection des données ») proposée par la CNIL et présentée dans le document 1.



Travail à faire

La première phase de la méthode PIA repose sur la compréhension du contexte.

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

➤ Documents 1 et 2

L'identification des menaces et des événements redoutés est un préalable à la cartographie des risques.

- Complétez le tableau d'analyse des scénarios de menaces présenté dans le document 4.

Justifiez les niveaux de vraisemblance retenus pour chaque menace.

➤ Fiches savoirs technologiques 1 et 2
➤ Documents 3 et 4

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

➤ Fiche savoirs technologiques 1
➤ Documents 3, 4 et 5

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

➤ Fiche savoirs technologiques 1

- 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.

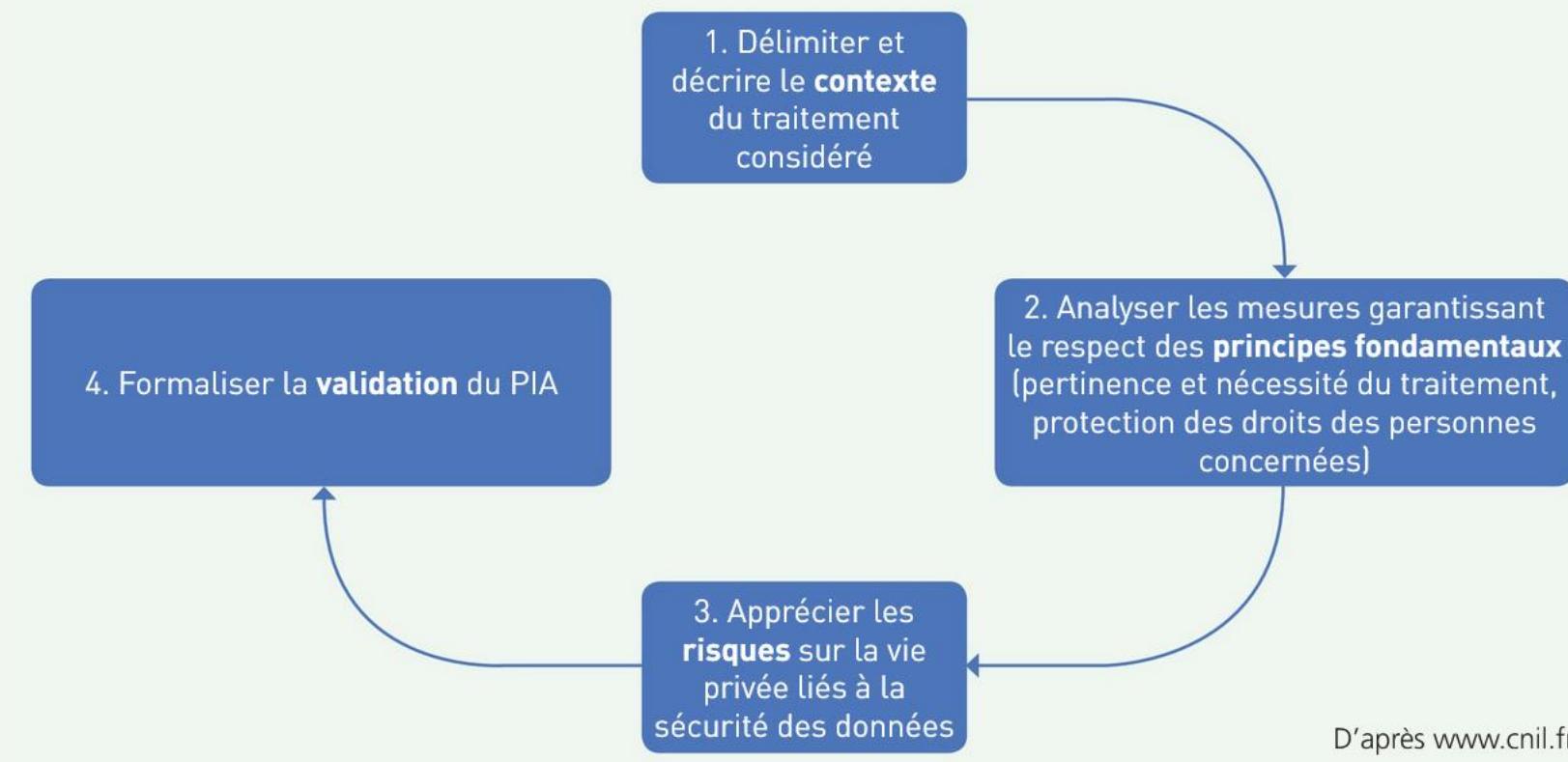
➤ Fiche savoirs technologiques 2

➤ Voir lexique BTS SIO, p. 221

Dossier documentaire

Document 1 Démarche PIA (*Privacy Impact Assessment*)

Une «analyse d'impact relative à la protection des données» (voir article 35 du RGPD), plus communément appelée *Privacy Impact Assessment* (PIA) décrit la manière d'employer la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité) préconisée par l'ANSSI. Quatre phases permettent de mener un PIA :



Document 2 Contexte du PIA relatif au traitement d'une étude de marché chez CentreCall

Le PIA porte sur le processus d'étude de marché mis en œuvre par CentreCall. M^{me} Azri est responsable du traitement des données manipulées dans le cadre de ce processus. L'objectif des études de marché est de collecter et d'analyser des informations qui identifient les caractéristiques d'un marché. Les données traitées sont ensuite mises à disposition des différents clients.

Données traitées
Informations personnelles, réponses au questionnaire, enregistrement audio de l'entretien, analyse des résultats de l'étude de marché.
Destinataires
• CentreCall. • Clients de l'étude de marché.
Durée de conservation
Les données sont conservées 1 an.

Cycle de vie des données

- Demande d'enregistrement de l'appel : la personne contactée notifie son acceptation ou non de l'enregistrement de l'entretien, et elle est informée des conditions de traitements de ses données à caractère personnel.
- Collecte des réponses aux questionnaires : les données sont collectées par l'opérateur par saisie sur son ordinateur de bureau, puis enregistrées sur un serveur de base de données hébergé par CentreCall.
- Vérification de l'enregistrement audio de l'entretien : l'enregistrement audio est vérifié puis sauvegardé sur un serveur de fichiers hébergé par CentreCall.
- Analyse des résultats de l'étude de marché.

Supports des données

- Un téléphone IP (*Internet Protocol*) est utilisé pour la conversation.
- Un ordinateur de bureau est mobilisé lors de l'enregistrement des réponses et de l'entretien.
- Plusieurs serveurs de base de données redondants stockent les réponses aux questionnaires, et un serveur de fichiers stocke l'enregistrement audio de l'entretien.

Missions professionnelles

Document 3 Risques identifiés sur les données à caractère personnel

Scénario 1

Usurpation d'un compte d'**authentification** d'un opérateur par un intervenant extérieur lors d'une opération de maintenance sur un ordinateur, pour récupérer des données confidentielles.

Les données se situent sur le serveur de base de données et non sur le poste de l'opérateur; la menace reste peu probable. Par contre, les données confidentielles peuvent bénéficier à une entité malveillante avec des conséquences importantes pour CentreCall.

Scénario 3

Consultation de données par un employé non-habilite due à une erreur de manipulation.

La consultation de données sans habilitation est peu probable, parce qu'une politique de sécurité rigoureuse dans ce domaine est mise en place par M^{me} Azri. Cependant, dans le cas d'une faiblesse temporaire dans ce domaine, les risques sont limités car le périmètre d'habilitation de chaque utilisateur est restreint.

Scénario 2

Suppression ou vol de données dans la base de données par un salarié mécontent, dans l'objectif de nuire à CentreCall, voire de les communiquer à un concurrent.

L'action est facile à mener avec des conséquences importantes.

Scénario 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.

Les serveurs de base de données sont actuellement peu protégés des menaces qui viendraient de l'extérieur de l'organisation. Une attaque de ce type provoquerait d'importantes conséquences, notamment sur la qualité et la crédibilité des futures synthèses d'études de marché.

Scénario 5

Arrêt du serveur de base de données par une attaque extérieure due à une multitude de requêtes.

Actuellement, le serveur de base de données pourrait être arrêté pour cette raison. Le risque serait alors maximal, car le travail de tous les opérateurs et des Call managers dépend de l'accès aux données hébergées sur le serveur.

Document 4 Analyse des scénarios de menaces

Source de menace	Type de menace	Bien support	Niveau de vraisemblance	Critères de sécurité		
				Confidentialité	Disponibilité	Intégrité
Scénario de menace lié au risque 1 : attaquant	Espionnage	Ordinateur de l'opérateur	2 : limité (les données ne sont présentes que sur le serveur de base de données)	L'authentification n'est plus assurée aux seules personnes habilitées.		
...				

Mesure de la vraisemblance : **1** négligeable – **2** limité – **3** important – **4** maximal.

Document 5 Événements redoutés

Exemple : scénario 1	Usurpation d'identité	Niveau de gravité : 3 (important). Les données confidentielles peuvent être exploitées par une entité malveillante.
...	...	

Mesure de la gravité : **1** négligeable – **2** limité – **3** important – **4** maximal.

➤ Voir lexique BTS SIO, p. 221

Travaux en laboratoire informatique

1

Recenser les traitements sur les données à caractère personnel au sein de l'organisation



La société Artemis souhaite bénéficier des services de CentreCall pour externaliser le processus de fidélisation de sa clientèle. M^{me} Azri, responsable des traitements chez CentreCall, profite de vos récents travaux sur la protection des données à caractère personnel et leurs traitements pour vous confier la charge de ce dossier. Un dossier documentaire est à votre disposition pour vous aider dans votre mission.

1. Schématissez 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.
➤ Logiciel JMOT à télécharger : www.lienmini.fr/6988-101
2. Identifiez les données à caractère personnel liées au processus de fidélisation.
3. Recensez les opérations réalisées sur les données à caractère personnel lors du processus de fidélisation.

Une déclaration des traitements réalisés sur des données à caractère personnel doit être effectuée auprès de la CNIL. Pour cela, un document numérique doit être complété par l'organisation.

M^{me} Azri a partiellement complété la déclaration pour la CNIL en indiquant les traitements réalisés sur les données à caractère personnel dans le cadre d'autres processus que celui du processus de fidélisation. Vous devez maintenant poursuivre la rédaction du document numérique de déclaration des activités de traitement. Pour cela, vous disposez de la liste des traitements complétée par M^{me} Azri (2^e onglet du registre numérique) et d'un modèle de fiche de registre pour enregistrer les informations liées au nouveau processus (3^e onglet).

4. À l'aide des documents 2 et 3, complétez le registre numérique des activités de traitement (2^e et 3^e onglets du document numérique) en tenant compte des réponses apportées aux questions précédentes pour le processus de fidélisation.
➤ Registre numérique des activités à compléter : www.lienmini.fr/6988-102

Document 1 Extrait de l'entretien entre M^{me} Azri et la société Artemis

M. Friand : Bonjour M^{me} Azri. Je suis Paul Friand, directeur de la société Artemis. Afin de nous recentrer sur notre cœur de métier, nous aimerais vous confier la charge du processus de fidélisation de nos clients. Pouvez-vous m'indiquer les éléments dont vous avez besoin pour cette prise en charge ?

M^{me} Azri : Bonjour M. Friand, je vous remercie pour la confiance que vous portez à notre entreprise. Nos centres d'appel, contrairement à un site vitrine, permettent d'apporter des réponses personnalisées et d'aider ainsi à gagner de nouveaux clients tout en conservant les clients actuels.

M. Friand : Quels sont les moyens mis en œuvre par votre entreprise pour optimiser cette fidélisation ?

M^{me} Azri : Nous disposons de trois atouts essentiels.

Premièrement, nos opérateurs sont formés sur vos produits et ils deviennent des conseillers qui défendent votre marque. Deuxièmement, nos équipes sont entourées de clientèles managers compétents qui mettent tous les moyens en œuvre pour accompagner les opérateurs dans leurs tâches au service de votre cause. Par exemple, ils vérifient que leur formation sur vos produits est à jour, ou encore ils contrôlent l'historique des échanges avec vos clients. Troisièmement, nous mobilisons une technologie qui permet un routage des demandes de vos clients vers l'opérateur le plus compétent pour y répondre.

M. Friand : Très bien. Pouvez-vous m'expliquer le processus que vous engagerez pour gérer la fidélisation de mes clients ?

...
M^{me} Azri : Chaque début de semaine, le clientèle manager en responsabilité du suivi de vos clients analyse sur notre logiciel spécifique les dates des derniers échanges. Si un client n'est pas entré en communication avec notre centre depuis plus de 6 mois, le clientèle manager va saisir cette information sur son logiciel et un opérateur sera désigné immédiatement pour appeler le client concerné.

M. Friand : Quelle sera l'approche adoptée par votre opérateur pour maintenir la fidélité de mon client ?

M^{me} Azri : L'opérateur va dans un premier temps, après acceptation de l'enregistrement de la communication, contrôler les informations personnelles de votre client : nom, prénom, adresse, numéro de téléphone, courriel.

Le cas échéant une modification de ses données sera réalisée dans notre base de données. Puis, dans un deuxième temps, il va demander à votre client son niveau de satisfaction par rapport à l'utilisation de vos produits et porter à sa connaissance l'actualité de votre marque, pour enfin lui proposer une éventuelle réduction commerciale.

M. Friand : Cela me semble parfait. Comment serai-je informé de l'évolution de vos relations avec les clients ?

M^{me} Azri : Tous les mois vous recevrez une synthèse de la part du clientèle manager. Ce sera le moment pour vous de nous indiquer les éventuels ajustements à adopter dans notre démarche ou propositions commerciales.

Document 2 Informations complémentaires

- Date de création de la fiche de registre : 15/09/2020
- Durée de conservation des données à caractère personnel : 1 an
- Mesures de sécurité des données : Protection du serveur de base de données par un pare-feu, sauvegardes régulières des données et accès aux données par authentification.

Document 3 Obligations pour le registre des traitements

Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité. Document de recensement et d'analyse, il doit refléter la réalité de vos traitements de données personnelles et vous permet d'identifier précisément :

- les parties prenantes (représentants, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données ;
- les catégories de données traitées ;
- à quoi servent ces données (ce que vous en faites), qui accède aux données et à qui elles sont communiquées ;
- combien de temps vous les conservez ;
- comment elles sont sécurisées.

www.cnil.fr

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



M^{me} Azri, vient de consulter le site de la CNIL. Elle a repéré une application qui permet de formaliser l'analyse d'impact relative à la protection des données (*Privacy Impact Assessment*). Elle vous demande de vous renseigner sur son utilisation et son utilité dans le cadre de l'analyse du traitement des données à caractère personnel liées aux études de marché.

ÉTAPE 1 Installation et analyse du paramétrage de l'outil

1. Téléchargez l'application PIA depuis le site de la CNIL.
➤ Outil PIA de la CNIL à télécharger : www.lienmini.fr/6988-103
2. Installez l'application et ouvrir l'exemple de PIA.
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.

ÉTAPE 2 Saisie des informations utiles pour le PIA

Pour cette étape, aidez-vous des informations présentées par les documents des deux missions réalisées précédemment (pp. 12 à 48).

4. Saisissez les informations relatives à la délimitation du contexte étudié (mission 2 - document 2, p. 17).
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 1, p. 17).
6. Enregistrez dans l'application PIA les mesures existantes pour la protection de la vie privée (mission 2 - document 2, p. 17).
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,

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

ÉTAPE 3 Analyse des résultats de l'étude des risques

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

Une évaluation des informations saisies doit être réalisée, en apportant des remarques qui permettent de déterminer un plan d'action afin de diminuer les impacts du traitement sur la protection des données à caractère personnel.

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.

Document 1 Règlement sur la protection de la vie privée chez CentreCall dans le cadre des études de marché

Proportionnalité et nécessité des traitements réalisés

Les personnes interrogées sont informées, dès le début de l'entretien téléphonique, que les données collectées dans le cadre d'une étude de marché sont stockées dans un serveur de base de données chez CentreCall et analysées pour le compte de clients clairement identifiés. Les traitements sont réalisés avec l'acceptation des conditions stipulées par les personnes interrogées. Seules les données qui permettent de mieux comprendre les besoins des clients sont collectées. Ces données ne sont pas anonymes. Une amélioration peut être envisagée en les rendant anonymes. L'ensemble des données collectées est régulièrement mis à jour lors du renouvellement des études sur un même marché.

Mesures protectrices des droits

Les personnes interrogées peuvent consulter le processus de traitement de leurs données à caractère personnel en consultant le site vitrine de CentreCall. Le consentement des personnes est obtenu au début de l'entretien, et il fait l'objet d'un enregistrement audio. Les personnes interrogées peuvent demander à CentreCall de fournir les informations collectées dans différents formats de fichier (CSV, XML, etc.). Les droits à l'effacement, à l'oubli, de limitation et d'opposition sont exercés par simple demande auprès de CentreCall. Il n'y a aucun sous-traitant et aucun transfert de données en dehors de l'Union européenne.

Document 2 Mesures pour la protection de la vie privée chez CentreCall dans le cadre des études de marché

Chiffrement	Le protocole SSL est utilisé pour le transfert des données entre l'ordinateur de l'opérateur et le serveur de bases de données.
Journalisation	L'ensemble des identifiants réseaux sont enregistrés dans un fichier journal (<i>log</i>) lors d'une demande d'accès aux serveurs de bases de données.
Archivage	Les données collectées lors des entretiens sont sauvegardées dans plusieurs serveurs de bases de données redondants avec un enregistrement sur un support externe tous les mois.

Fiche savoirs technologiques 1

La typologie des risques et leurs impacts

I

Définitions de vulnérabilité, menace et risque

Vulnérabilité	Menace	Risque
En informatique, une vulnérabilité est une faiblesse de la sécurité du système d'information (SI) qui peut affecter son fonctionnement normal.	Une menace est une cause intentionnelle ou non-intentionnelle qui peut entraîner des dommages sur le SI.	Un risque de sécurité du SI est la probabilité de l'exploitation d'une vulnérabilité du SI par une menace. Le niveau d'un risque est estimé en fonction de sa gravité et de la vraisemblance de son apparition.

Les objectifs de la sécurité informatique consistent à limiter les vulnérabilités du SI.

II

La typologie des risques informatiques

1. La méthode EBIOS

- EBIOS Risk Manager : www.lienmini.fr/6988-104
- Fiche méthode 5, p. 211

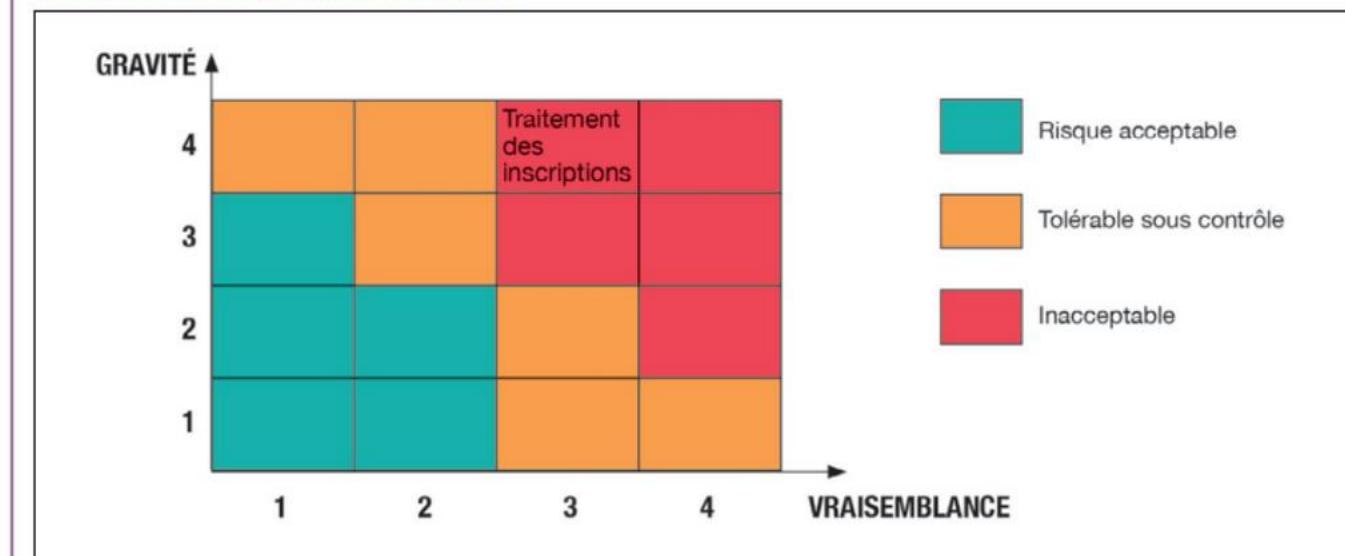
La méthode EBIOS Risk Manager (Expression des besoins et identification des objectifs de sécurité) développée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et retenue par la CNIL (Commission nationale de l'informatique et des libertés) permet d'identifier et de hiérarchiser les différents risques dans un contexte clairement défini.

Un risque est défini par l'ANSSI comme « un scénario qui combine un événement redouté et un ou plusieurs scénarios de menaces ». Un événement redouté désigne par exemple la possibilité d'atteindre des données avec des conséquences probables sur la vie privée des personnes concernées.

2. L'évaluation des risques

L'évaluation des impacts des risques informatiques est réalisée par le croisement de son niveau de vraisemblance et de gravité.

Exemple de cartographie des risques



La vraisemblance reflète la probabilité ou la possibilité que l'un des modes opératoires de l'attaquant aboutisse à l'objectif visé. Elle dépend des vulnérabilités des supports face aux menaces et des capacités des sources de risque à les exploiter.

La gravité évalue l'enjeu d'un événement redouté sur des «valeurs métier», c'est-à-dire stratégiques pour l'organisation (informations confidentielles, processus métier, matériels, logiciels, etc.).

Exemple de mesure de la gravité

Valeur métier	Évènement redouté	Impacts	Gravité
Facturation	Altération des informations sur les factures	<ul style="list-style-type: none"> • Impossibilité de recevoir un paiement • Perte de crédibilité • Impossibilité de remplir les obligations légales 	G3 - Grave

III Les impacts des risques informatiques

L'ANSSI, au travers de sa méthode EBIOS, identifie différentes catégories d'impacts.

Impacts sur les missions et les services de l'organisation	Conséquences directes ou indirectes sur la réalisation des missions et services.
Impacts humains, matériels ou environnementaux	<ul style="list-style-type: none"> • Impacts sur la sécurité ou sur la santé des personnes : conséquences sur l'intégrité physique de personnes. • Impacts matériels : dégâts matériels ou destruction de biens supports. • Impacts sur l'environnement : conséquences écologiques à court ou long terme.
Impacts sur la gouvernance	<ul style="list-style-type: none"> • Impacts sur la capacité de développement ou de décision : conséquences sur la liberté de décider, de diriger, de mettre en œuvre la stratégie de développement. • Impacts sur le lien social interne : conséquences sur la qualité des liens sociaux au sein de l'organisation. • Impacts sur le patrimoine intellectuel ou culturel : conséquences sur les connaissances non-explicites accumulées par l'organisation sur le savoir-faire, les capacités d'innovation, les références culturelles communes.
Impacts financiers	Conséquences pécuniaires.
Impacts juridiques	Conséquences suite à une non-conformité légale, réglementaire, normative ou contractuelle.
Impacts sur l'image et la confiance	Conséquences sur l'image de l'organisation, la notoriété, la confiance des clients.

Fiche savoirs technologiques 2

Les principes de la sécurité

La sécurité des systèmes d'information repose sur quatre principes fondamentaux :



I

La confidentialité

La **confidentialité** vise à assurer que les données ne sont accessibles qu'aux seules personnes autorisées.

Exemple : la connexion d'un utilisateur au réseau de l'organisation par son identifiant et son mot de passe personnel ne donne accès qu'aux données qu'il est autorisé à consulter ou à modifier.

II

La disponibilité

La **disponibilité** doit rendre les données accessibles et utilisables par les personnes autorisées sans interruption.

Exemple : la redondance des connexions réseaux permet d'accéder aux données de manière continue, même si une connexion est rompue.

III

L'intégrité

Le principe d'**intégrité** s'assure que les données ne peuvent pas être modifiées pendant leur transfert, leur traitement ou leur stockage.

Exemple : des protocoles de cryptage, comme le protocole SSL, permettent de s'assurer que les données ne sont pas modifiées pendant leur transfert sur le réseau.

IV

La preuve

Le principe de non-réputation consiste à apporter la preuve non réfutable d'un acte malveillant. La non-réputation est assurée par la combinaison de trois éléments : l'authentification, l'imputabilité et la traçabilité.

Authentification	Imputabilité	Traçabilité
L'authentification permet de s'assurer de la légitimité de la demande d'accès, et d'accorder les droits associés à celle-ci. La saisie d'un identifiant et d'un mot de passe peut être une solution d'authentification.	L'imputabilité désigne la possibilité d'attribuer la responsabilité d'un acte à une personne clairement identifiée.	La traçabilité permet de fournir un historique de l'utilisation d'un système d'information pour disposer d'une preuve des actions menées sur des données.

Exemple : en cas d'action malveillante sur un service informatique de l'organisation, le fichier de journalisation (*log*) doit permettre de prouver qui est intervenu et sur quel service, afin d'apporter la preuve de l'acte.

Fiche savoirs technologiques 3

Sécurité et sûreté

I

Définitions

La sûreté vise à prévenir les risques et conséquences d'un événement accidentel ou involontaire.

La sécurité consiste à prévenir les actes de malveillance en combinant des moyens humains, techniques et organisationnels. Cette notion est souvent englobée dans le terme de sûreté informatique. Elle doit permettre de faire face aux risques de vol de données, d'intrusion dans le système informatique, ou d'effectuer la recherche de dégradation de service du SI.

II

Les périmètres respectifs

1. Le périmètre de la sûreté informatique

a. Les menaces non intentionnelles

Le périmètre de la sûreté informatique englobe les menaces non intentionnelles qui sont, par définition, peu prévisibles et non-volontaires.

b. Les types de menaces

Menace d'accident naturel	Menace humaine	Menace liée au matériel
Un risque naturel (orage, inondation, etc.) est un élément imprévu ou difficilement prévisible qui peut être dangereux lorsqu'il impacte une vulnérabilité du SI.	L'erreur humaine, la maladresse ou la négligence peuvent mettre à jour une faiblesse du SI et mettre en échec sa stabilité.	Le choix du matériel informatique peut rendre plus ou moins vulnérable le SI. La réduction de certains coûts d'acquisition peut être source de menaces pour le SI.

2. Le périmètre de la sécurité informatique

a. Les menaces délibérées

Le périmètre de la sécurité informatique regroupe les menaces délibérées qui proviennent de personnes malveillantes, et qui peuvent nuire au SI. Ces personnes sont internes ou externes à l'organisation, et disposent de capacités plus ou moins importantes dans les possibilités de détérioration du SI, selon leur niveau de compétence technique et leurs droits d'accès au SI.

b. Les catégories d'attaquants

D'après l'ANSSI, les profils des attaquants peuvent être regroupés selon trois grandes catégories :

- les organisations structurées guidées par une logique d'efficacité et de gain disposant de moyens sophistiqués et conséquents, voire quasi illimités (États, crime organisé) ;
- les organisations ou groupes guidés par une motivation idéologique disposant de moyens significatifs mis en œuvre de façon relativement coordonnée (terroristes, activistes) ;
- les attaquants disposant de moyens limités mais spécialisés (individus isolés, groupes d'individus).

3. Les principaux types de menaces

Quatre principaux types de menaces sont mis en avant par l'ANSSI : la déstabilisation, l'espionnage, le sabotage et la cybercriminalité.

Menaces	Types d'attaques
Déstabilisation	<ul style="list-style-type: none"> Déni de service : action qui rend un service inaccessible, par l'envoi d'une multitude de requêtes vers un serveur pour provoquer sa panne ou sa dégradation. Défiguration : ajout ou remplacement des pages d'un site Web afin de revendiquer un message idéologique. Divulgation de données : récupération de données confidentielles d'une organisation en exploitant une vulnérabilité du réseau informatique.
Espionnage	<ul style="list-style-type: none"> Attaque par « point d'eau » (<i>wateringhole</i>) : infection du site Internet d'une organisation pour contaminer les ordinateurs des visiteurs, afin d'accéder au réseau de l'organisation. Attaque par hameçonnage ciblé (<i>spearfishing</i>) : usurpation de l'identité d'une personne connue du destinataire pour envoyer un message ciblé à un membre d'une organisation, afin de lui faire ouvrir une pièce jointe malveillante qui permettra d'accéder au réseau de l'organisation.
Sabotage	Les modes d'attaques sont nombreux, mais ils visent tous à créer une panne dans un périmètre ou sur l'ensemble du système d'information d'une organisation.
Cybercriminalité	<ul style="list-style-type: none"> Rançongiciel (<i>ransomware</i>) : données confidentielles rendues inaccessibles jusqu'au paiement d'une rançon. Le chantage peut parfois toucher des données gênantes, que l'on menace de rendre publiques sur Internet. Hameçonnage (<i>phishing</i>) : action visant à tromper un utilisateur pour l'inciter à communiquer des données personnelles, souvent des données bancaires. Les formes peuvent être diverses, telles que l'utilisation des réseaux sociaux, un courriel ou encore un SMS.

D'après www.ssi.gouv.fr

Fiche savoirs CEJM appliquée 1

Les traitements sur les données à caractère personnel

I Les données à caractère personnel

1. Définition

La CNIL définit une donnée à caractère personnel comme : « Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification, dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

Article 2 de la loi n° 78-17 du 6 janvier 1978.

2. La responsabilité de l'organisation

Une personne peut être directement identifiée par son nom de famille, mais elle peut également l'être, de manière indirecte, par d'autres éléments tels qu'un enregistrement vocal ou une photographie.

Le responsable de traitement a la responsabilité de mener une politique de sécurité permettant le respect des principes fondamentaux en matière de protection des données à caractère personnel (voir FS CEJMA 2 – Chapitre 2, p. 33).

Les coordonnées d'une organisation ne sont pas considérées comme des données à caractère personnel.

II Le traitement des données à caractère personnel

1. Définition

La CNIL définit un traitement de données à caractère personnel comme « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

Article 2 de la loi n° 78-17 du 6 janvier 1978

2. Les opérations concernées

Des opérations variées peuvent donc être considérées comme des traitements au sens de la CNIL. Il s'agit, pour chaque organisation, d'identifier ces opérations à l'intérieur d'un processus clairement défini (exemple : la gestion des formations) afin de repérer les vulnérabilités dans la protection des données à caractère personnel.

Un traitement n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions. Un fichier de données à caractère personnel est constitué d'un ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

Un traitement de données doit avoir un objectif, c'est-à-dire une finalité déterminée.

Exemple : la collecte des coordonnées personnelles des salariés d'une organisation a pour finalité de traiter la gestion des salaires.

1 QCM



Retrouvez ce QCM
en version interactive
www.lienmini.fr/6988-105

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

Applications

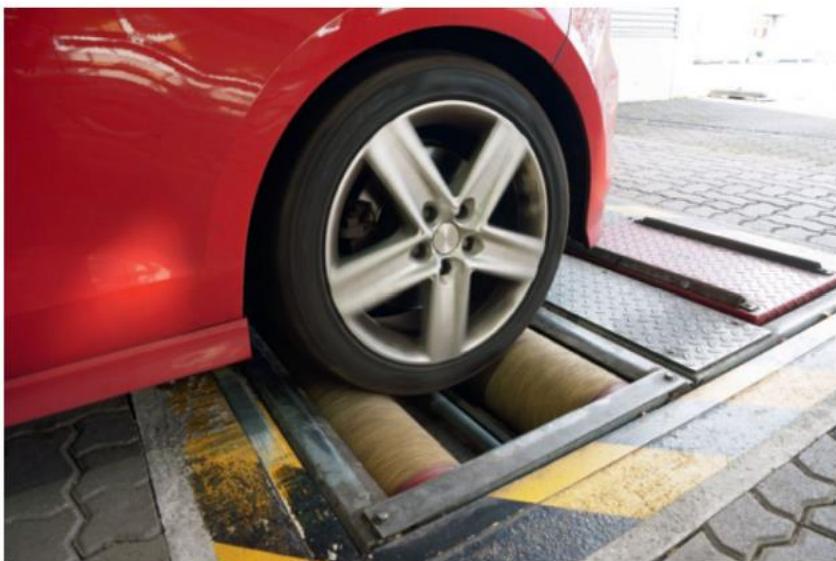
2

Analyser un PIA



› Fiche savoirs technologiques 1

Situation



La société Testop, située à Lille, est spécialisée dans la fabrication de bancs de tests pour l'industrie automobile. M. Grospire, responsable des traitements, vient de finaliser la saisie des éléments relatifs à l'analyse d'impact sur la protection des données à caractère personnel concernant le processus de recrutement de ses salariés. Il vous demande de compléter, sur l'application PIA développée par la CNIL, les mesures envisageables pour limiter les risques mentionnés.

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

› PIA : www.lienmini.fr/6988-106

- 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.
- 3 Affichez et commentez la cartographie des risques.

Vous devez maintenant activer, dans l'application PIA, une demande d'évaluation pour les items liés aux risques :

- mesures existantes ou prévues ;
- accès illégitime à des données ;
- modification non désirée de données ;
- disparition de données.

- 4 Évaluez les différents items en proposant, le cas échéant, des mesures correctrices envisageables.
- 5 Commentez l'évolution de la cartographie des risques sur les données à caractère personnel.

3

Cartographier le traitement des données à caractère personnel



› Fiche savoirs technologiques 1

- 1 Après avoir visionné la vidéo, expliquez en quoi consiste la cartographie des traitements des données personnelles et quels sont ses enjeux.
- 2 Pourquoi le registre des traitements des données à caractère personnel est-il une étape préalable à la cartographie des traitements ?

VIDÉO

Cartographier le traitement des données



www.lienmini.fr/6988-107

4

Repérer l'utilisation des données à caractère personnel



➤ Fiche savoirs technologiques 2

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



Annexe

Extrait de la politique de protection de la confidentialité des données personnelles de Castorama

Nous appartenons au groupe Kingfisher comprenant B&Q, Screwfix, Castorama et Brico Dépôt (pour plus d'information : www.kingfisher.com).

Nous pouvons partager vos données personnelles avec d'autres entités du groupe Kingfisher. Il est également possible que les entités du groupe Kingfisher utilisent les données personnelles que nous partageons avec eux pour améliorer leurs sites web et d'autres services numériques, à des fins d'analyse ainsi que pour vous proposer des produits et des services susceptibles de vous intéresser.

Nous pouvons partager les données que nous détenons à votre sujet (par exemple votre email

et des informations concernant vos achats) avec des tiers qui détiennent également des données vous concernant dans le but de vous identifier et pour nous permettre (ou les sociétés du groupe Kingfisher ou d'autres tiers en notre nom) de vous offrir des renseignements marketing pertinents. [...]

Nous pouvons transmettre des données personnelles à nos assureurs dans le cas où une action est ou pourrait être intentée contre nous. [...]

Nous pouvons partager des données anonymes ou agrégées (telles que des statistiques agrégées ou d'autres données anonymes) avec des tiers.

www.castorama.fr

5

Traitements et risques sur les données à caractère personnel



➤ Fiche savoirs technologiques 2

- 1** Après avoir visionné la vidéo, repérez les différents moyens de collecte, stockage et diffusion des données à caractère personnel.
- 2** Quels sont les traitements des données à caractère personnel présentés ?
- 3** Listez les obligations légales rappelées dans la vidéo.
- 4** Indiquez les sanctions encourues par les entreprises en cas de non-respect de la sécurité des données à caractère personnel.

VIDÉO

Le traitement des données



www.lienmini.fr/6988-108

6 Dissocier les notions de sécurité et de sûreté informatique



➤ Fiche savoirs technologiques 3

- 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	<input type="checkbox"/>	<input type="checkbox"/>	
Les données d'un hôpital sont illisibles à la suite d'une attaque de type <i>ransomware</i> .	<input type="checkbox"/>	<input type="checkbox"/>	
L'apparence du site vitrine d'une entreprise est modifiée pendant un week-end par des personnes malveillantes.	<input type="checkbox"/>	<input type="checkbox"/>	
Une surcharge électrique temporaire due à des travaux réalisés dans les bâtiments de la société provoque une panne des routeurs.	<input type="checkbox"/>	<input type="checkbox"/>	

7 Identifier les données à caractère personnel



➤ Fiche savoirs CEJMA 1

- 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	<input type="checkbox"/> oui <input type="checkbox"/> non	
L'adresse courriel professionnelle d'un directeur des services informatiques	<input type="checkbox"/> oui <input type="checkbox"/> non	
Une photo postée sur un réseau social	<input type="checkbox"/> oui <input type="checkbox"/> non	
Une vidéo de présentation de son parcours professionnel envoyée à une entreprise dans le cadre d'un recrutement	<input type="checkbox"/> oui <input type="checkbox"/> non	
Les coordonnées GPS de localisation d'un smartphone	<input type="checkbox"/> oui <input type="checkbox"/> non	
Le groupe sanguin d'un patient stocké sur le serveur de base de données de son médecin	<input type="checkbox"/> oui <input type="checkbox"/> non	
Les enregistrements de vidéosurveillance d'un datacenter	<input type="checkbox"/> oui <input type="checkbox"/> non	
Le numéro d'enregistrement au registre du commerce et des sociétés d'une entreprise	<input type="checkbox"/> oui <input type="checkbox"/> non	
Le numéro de sécurité sociale d'un salarié saisi sur sa fiche d'embauche	<input type="checkbox"/> oui <input type="checkbox"/> non	

Appliquer et diffuser la réglementation liée aux données à caractère personnel

COMPÉTENCES

- Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel
- Sensibiliser les utilisateurs à la protection des données à caractère personnel

SAVOIRS ASSOCIÉS

- Les données à caractère personnel : définition, réglementation, rôle de la CNIL

Situation professionnelle

L'étude des **risques** liés au traitement des données à caractère personnel menée par la direction du service informatique de CentreCall démontre qu'une démarche de sensibilisation doit être réalisée, notamment auprès des opérateurs téléphoniques et de leurs managers. En outre, il apparaît que les derniers changements réglementaires amènent CentreCall à répondre à de multiples

questions de ses clients et des personnes contactées dans le cadre des études de marché.

Mme Azri vous demande de vérifier que les actions menées sur les données à caractère personnel sont conformes à la législation, puis de réaliser une campagne de sensibilisation à destination des opérateurs téléphoniques et de leurs managers.



➤ Voir présentation générale, p. 49

Missions professionnelles

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

La charte de protection des données personnelles est publiée sur le site vitrine de CentreCall. Elle informe les visiteurs sur le traitement de leurs données. Un espace personnel peut être créé à la demande des personnes interrogées, où elles peuvent visualiser les données collectées par les opérateurs téléphoniques. Cependant, de nombreuses questions sont postées dans la rubrique de contact par messagerie, dont certaines soulèvent des problèmes de conformité avec la législation. Une récente notification de la **CNIL** inquiète plus particulièrement M^{me} Azri. Pour cette mission, vous êtes chargé(e) de vérifier la conformité de la politique de protection des données personnelles de CentreCall avec la réglementation en vigueur, et d'apporter des réponses aux questions des internautes.



Travail à faire

- 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**.

- > Fiche savoirs CEJMA 2
- > Document 1

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

- > Fiche savoirs CEJMA 2
- > Document 2

M^{me} Azri souhaite que vous apportiez une réponse rapide et argumentée au courriel d'une personne récemment interrogée par l'un des centres d'appels, ainsi qu'au courrier d'avertissement reçu de la CNIL.

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

- > Document 3

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

- > Documents 4 et 5

M^{me} Azri décide, pour des raisons financières, d'externaliser une partie des traitements réalisés sur les données à caractère personnel collectées dans le cadre des études de marché. Son choix s'oriente vers la société Osiris, basée en Inde.

- 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.

- > Fiche savoirs CEJMA 2
- > Document 6

> Voir lexique BTS SIO, p. 221

Dossier documentaire

Document 1 Extrait de la charte de confidentialité publiée sur le site de CentreCall

La publication de notre politique de confidentialité vous informe des finalités des traitements réalisés sur les données que vous nous communiquez.

CentreCall s'engage à assurer le meilleur niveau de protection de vos données personnelles, en conformité avec les réglementations européennes et françaises en vigueur.

CentreCall utilise vos données personnelles pour les finalités suivantes

- La réalisation d'études de marché pour le compte de nos clients

Nous recueillons les informations suivantes pour la réalisation des études de marché : vos coordonnées, vos motivations pour l'achat d'un produit ou d'un service.

- L'externalisation de l'accueil téléphonique de nos clients

Les appels téléphoniques reçus ou émis pour le compte de clients peuvent faire l'objet d'enregistrements audio.

- La sécurité de notre site

Nous collectons certaines données de navigation afin d'assurer la sécurité de nos services et de détecter, éviter ou retracer toute tentative de malveillance, intrusion informatique ou violation des conditions d'utilisation de ces services.

- La personnalisation des publicités en ligne

Nous pouvons utiliser des données qui ne permettent pas de vous identifier directement (identifiants techniques ou données sociodémographiques) afin d'adapter la publicité que vous visualisez sur notre site ou sur ceux de nos partenaires. Vos données peuvent être croisées avec d'autres données de navigation collectées à l'occasion de nos relations avec des partenaires. Pour plus d'informations et le suivi de vos cookies, rendez-vous à la page «cookies» du site.

Quelles sont les données personnelles collectées ?

Du fait de vos échanges avec nos opérateurs téléphoniques ou de votre inscription sur notre site, nous collectons et traitons les données suivantes : vos nom, prénom, adresse, adresse courriel, mot de passe, numéro de téléphone, préférences et centres d'intérêts, enregistrements de conversation.

Comment est assurée la sécurité des données personnelles ?

La protection de la confidentialité et de l'intégrité de l'ensemble des données à caractère personnel collectées par notre organisation est assurée par la mise en place de plusieurs dispositifs :

- un pare-feu certifié ANSSI assure le filtrage et la détection des tentatives d'intrusions ;
- l'ensemble de nos serveurs de données sont répliqués pour permettre, en cas de perte de données, une restauration sécurisée et rapide ;
- les applications développées par nos services pour collecter et traiter les données à caractère personnel intègrent des solutions qui sécurisent les flux d'informations et évitent des actes malveillants.

Missions professionnelles

Document 2 Durée de conservation des données personnelles chez CentreCall

Finalité du traitement	Base légale	Durée de conservation en base opérationnelle	Archivage	Observations utiles
Réalisation d'études de marché		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		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		3 ans à compter de l'inscription sur une liste d'alerte	2 ans	Certaines données peuvent être collectées et conservées afin de vérifier l'identité réelle de la personne interrogée.
Publicité ciblée ; profilage publicitaire		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.

Document 3 Courriel de demande de suppression de données personnelles

Message **Options**

Expéditeur :	Maurice Bleuet
Objet :	Demande de suppression de données personnelles
Date :	10/11/2011
Destinataire :	contact@centrecall.fr

Bonjour,

Suite à un échange avec mon entourage, je regrette de vous avoir communiqué certaines informations dans le cadre de votre étude de marché relative à la consommation de boissons alcoolisées. Je ne retrouve pas dans votre politique de protection des données personnelles la procédure à suivre pour demander la suppression de ces données. Pourriez-vous m'informer sur cette démarche ?

Cordialement,

Maurice Bleuet

➤ Voir lexique BTS SIO, p. 221

Document 4 Avertissement de la CNIL à CentreCall

Madame Azri,

Lors de notre dernier contrôle dans vos locaux, nous avons constaté que votre pare-feu présentait de nombreuses alertes concernant des intrusions, depuis Internet, sur certains de vos serveurs hébergeant des données personnelles.

Cela traduit un manquement aux dispositions de la loi Informatiques et Libertés, en particulier celles relatives aux données personnelles des personnes interrogées.

Nous attendons de votre part une information sur les mesures que vous comptez mettre en place pour remédier à ce manquement.

M. Bromont

Responsable de la protection des données personnelles à la CNIL.

Document 5 Solution pour la protection technique des accès aux données personnels proposée par le stagiaire de la DSI à M^{me} Azri

Suite aux récentes alertes d'intrusions dans notre réseau, voici la solution que nous envisageons de mettre en place.

Installation du pare-feu Stormshield SN510, qui dispose des caractéristiques techniques suivantes :

- activation de l'archivage des *logs* en local sur notre «appliance» (matériel et logiciel intégré), conforme aux exigences réglementaires de conservation des traces de communications Internet ;
- fonction de **proxy cache HTTP** qui améliore la consommation de **bande passante** lors de la navigation ;
- fonctionnalités réseau avancées des appliances *Stormshield Network Security*, qui s'adaptent à notre infrastructure, en toute transparence et sans impact ;
- système de prévention d'intrusion (**IPS**, *intrusion prevention system*) qui permet de prendre des mesures afin de diminuer les impacts d'une 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. Les IPS peuvent donc parer les attaques connues et inconnues.

Document 6 Réponse de la société Osiris à la demande d'information de CentreCall

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

Les données personnelles sont stockées dans un lieu hautement protégé par notre pare-feu, et les flux des traitements réalisés sur ces données sont isolés des autres. Notre personnel est formé au respect de la confidentialité lors des traitements réalisés avec ce type de données.

Toutes nos applications utilisées pour les traitements des données à caractère personnel sont développées dans le respect de la législation européenne. Elles sont régulièrement auditées par des organismes européens indépendants.

Osiris garantit dans son SI :

- le chiffrement des données stockées ;
- le chiffrement des transmissions de données (connexion de type HTTPS et **VPN**) ;
- la **traçabilité** des opérations (journaux, audits) et la gestion des **habilitations** ;
- une haute **disponibilité** de l'ensemble de notre infrastructure.

Missions professionnelles

2

Sensibiliser les utilisateurs à la protection des données à caractère personnel

Les nombreuses irrégularités constatées imposent de mettre en place une campagne de sensibilisation sur la protection des données personnelles, à destination des opérateurs téléphoniques et de leurs managers.

Vous participez à l'élaboration et à la vérification des documents qui seront mobilisés pour cette campagne.



Travail à faire

M^{me} Azri vous demande de sensibiliser vos collègues à la protection des données à caractère personnel à l'aide d'une charte informatique. Elle vous communique un extrait du projet qu'elle vient de rédiger.

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.
➤ Documents 1 et 2
2. Expliquez en quoi la publication de la charte informatique peut constituer un élément de sensibilisation des collaborateurs de CentreCall.
3. Proposez d'autres supports de communication qui pourraient être réalisés dans le cadre de cette campagne de sensibilisation.

Afin de faciliter l'adhésion des *call managers* à la campagne de sensibilisation, vous les amenez à s'interroger sur la manière d'optimiser l'application du RGPD dans leur centre d'appel.

4. Retrouvez comment CentreCall peut améliorer son fonctionnement grâce au RGPD.
➤ Document 3

Dossier documentaire

Document 1 Extrait du projet de charte informatique

RÈGLES DE PROTECTION DES DONNÉES PERSONNELLES

1. Domaine d'application de la charte

Les règles décrites dans la présente charte s'appliquent à tout le personnel utilisant les moyens informatiques de CentreCall, ainsi que tout autre moyen de connexion à distance, afin d'accéder *via* Internet à tout service ou traitement électronique interne ou externe de l'entreprise, y compris l'accès à Internet. Le non-respect d'une de ces règles est susceptible d'entrainer des mesures disciplinaires internes voire, en cas de violation d'un texte législatif ou réglementaire, des poursuites judiciaires. Les diverses lois concernant ce domaine sont présumées connues.

2. Conditions d'accès de l'utilisateur

- L'utilisation des ressources informatiques de l'entreprise est soumise à autorisation préalable.
- Cette autorisation est concrétisée par l'ouverture d'un compte utilisateur (création d'un courriel et d'un identifiant pour l'accès au réseau de l'entreprise).
- Cette autorisation est strictement personnelle et ne doit en aucun cas être cédée, même temporairement, à un tiers.
- Cette autorisation ne vaut que pour les activités conformes aux missions de l'entreprise, dans le respect de la législation en vigueur.
- L'entreprise se réserve le droit de retirer à tout moment cette autorisation et ce, sans préavis.
- Chaque utilisateur doit user raisonnablement des ressources partagées auxquelles il accède.
- L'usage de ces ressources est, pour l'essentiel, dédié à des utilisations professionnelles.
- L'usage personnel doit rester limité.

3. Respect de la confidentialité des informations

- Les utilisateurs ne doivent pas tenter de lire, copier, divulguer ou modifier les fichiers d'un autre utilisateur sans y avoir été autorisés.
- Les utilisateurs doivent s'interdire toute tentative d'interception de communications entre tiers.
- Les utilisateurs sont tenus à la réserve d'usage sur toute information relative au fonctionnement interne de l'entreprise.
- Les utilisateurs sont tenus de prendre, avec l'aide éventuelle du service informatique et du **DPO** (*Data Protection Officer*, délégué à la protection des données), les mesures de protection des données nécessaires au respect des engagements de confidentialité pris par l'entreprise vis-à-vis de tiers.
- Une attention toute particulière doit être portée à la confidentialité des bases de données CentreCall. Leur utilisation doit respecter les engagements de CentreCall.

Document 2 Valeur de la charte informatique

La charte informatique a la même valeur que le règlement intérieur si elle est adoptée en respectant les formalités et les règles de fond applicables par celui-ci (comme par exemple la consultation préalable des représentants du personnel). Si elle est insérée au règlement intérieur, cela implique que celui-ci soit modifié en respectant les prescriptions du Code du travail.

Missions professionnelles

Document 3 La législation sur la protection des données, une opportunité pour les entreprises

La législation sur la protection de la vie privée présente des exigences strictes et fait encourir de lourdes peines à ceux qui voudraient s'en affranchir ; elle est ainsi parfois perçue comme un fardeau, alors qu'il faut pourtant y voir là un véritable moteur, capable de dynamiser la croissance d'une organisation.

Optimiser les processus business

Les règles de confidentialité entraînent une plus grande transparence sur la collecte des données. Bien que les textes de loi ne les obligent pas tous à informer explicitement les clients de l'utilisation qui est faite de leurs informations personnelles, les entreprises doivent néanmoins procéder à un audit approfondi pour comprendre quel type de données elles stockent et pour quelle raison ; l'occasion aussi pour les organisations de se demander pourquoi elles collectent ces informations, si elles les exploitent efficacement et comment optimiser leur utilisation. Cette compréhension approfondie du flux de données offre une plus grande visibilité des **processus métiers**, et permet d'en tirer le meilleur parti.



Améliorer la gestion des données pour une meilleure rentabilité

Une fois qu'une entreprise a analysé l'ensemble de ses données, il est important qu'elle se pose la question suivante : « ai-je besoin de tout ? » Et la réponse sera très probablement « non ». Ainsi, un contrôle continu dans un souci de conformité est un excellent moyen

d'éliminer toutes les données superflues, telles que des fichiers redondants, obsolètes et inutiles, qui n'ont pas d'intérêt stratégique réel pour l'entreprise. En nettoyant les référentiels, il est également possible de réduire les coûts de traitement et de stockage des données, de mieux anticiper les éventuels frais si elles sont stockées dans le *cloud* et d'allouer le budget de façon plus pertinente. [...]

Réorganiser la stratégie de sécurité

Le coût lié aux failles de sécurité et au temps d'arrêt de l'activité d'une organisation suite à un vol de données critiques continue d'augmenter. Une raison supplémentaire, au-delà du respect de la législation, d'encourager les entreprises à revoir leur politique de sécurité. Il est en effet presque impossible de ne protéger que les données réglementaires et de laisser le reste de l'infrastructure informatique en dehors du périmètre surveillé. Par conséquent, une organisation doit établir un contrôle strict de son activité dans l'intégralité de son environnement informatique, afin de mieux comprendre les risques qui s'y rapportent. À long terme, cela permettra d'investir davantage dans des ressources liées à la sécurité et de diminuer le risque d'**incidents** graves.

Pierre-Louis Lussan (*country manager France, Netwrix*¹)
www.lesechos.fr, 17 juin 2019

1. Netwrix est un éditeur privé de logiciels de sécurité informatique.

Travaux en laboratoire informatique

Concevoir une journée de formation sur la protection des données à caractère personnel



Chaque utilisateur du système d'information est un maillon d'une chaîne : la défaillance de l'un d'entre eux compromet toute la chaîne. D'où l'importance de tous les sensibiliser à la protection des données à caractère personnel. Ainsi, CentreCall met en place une journée de formation destinée aux nouveaux opérateurs téléphoniques. Cette formation est organisée en deux ateliers : la sensibilisation à la protection des données à caractère personnel (atelier 1) et la présentation de la politique de protection des données personnelles de CentreCall (atelier 2).

Vous êtes en charge de la conception de cette session de formation et de l'élaboration de supports adaptés aux stagiaires.



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.
➤ [Documents 1 et 2](#)
2. Choisissez l'approche pédagogique la plus appropriée pour chaque atelier. Justifiez.

ÉTAPE 2 Préparation des supports de l'atelier 1

Pour faciliter l'écoute des nouveaux opérateurs téléphoniques, un scénario d'immersion a été imaginé. Pour la mise en œuvre du scénario proposé, vous devrez utiliser le logiciel VirtualBox en vous appuyant sur la fiche méthode 3.

3. Testez le scénario d'immersion des opérateurs téléphoniques en respectant le cahier des charges présenté dans le document 3.
➤ [Fiche méthode 3, p. 207](#)
➤ [Document 3](#)
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 ?
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.
➤ [Document 4](#)

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.
➤ [Document 5](#)

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.
➤ [Document 6](#)

Document 1 Organisation de la journée de formation

8 h 00 – 9 h 00	Accueil des nouveaux opérateurs téléphoniques.
9 h 00 – 12 h 00	Atelier 1. Sensibilisation à la protection des données à caractère personnel.
14 h 00 – 17 h 00	Atelier 2. Présentation de la politique de protection des données personnelles de CentreCall.
17 h 00 – 17 h 30	Évaluation de la formation.

Document 2 Processus de préparation d'une session de formation**Définition des objectifs de la formation**

Les objectifs de la formation doivent être clairement identifiés avant l'intervention, afin de faciliter la cohérence entre le message diffusé, les supports mobilisés et l'évaluation des acquis. Un cahier des charges de la formation, comprenant les messages à véhiculer et le déroulé de la formation, doit être rédigé avant l'intervention.

Prise en compte des «qualités des apprenants»

La «qualité des apprenants» revêt deux dimensions : leur personnalité et leurs prérequis quant au sujet de la formation. Le formateur doit en tenir compte pour ne pas se retrouver décalage avec son public.

La personnalité peut être appréhendée pendant les premiers moments de l'intervention, afin d'adapter son discours.

Les prérequis doivent être analysés en amont de l'intervention par un diagnostic du niveau de connaissance des apprenants sur le sujet à traiter.

Adaptation de l'approche pédagogique au public visé

L'étape précédente doit aider le formateur à adopter une position face à son public. Plusieurs approches peuvent être mobilisées, dont les deux suivantes :

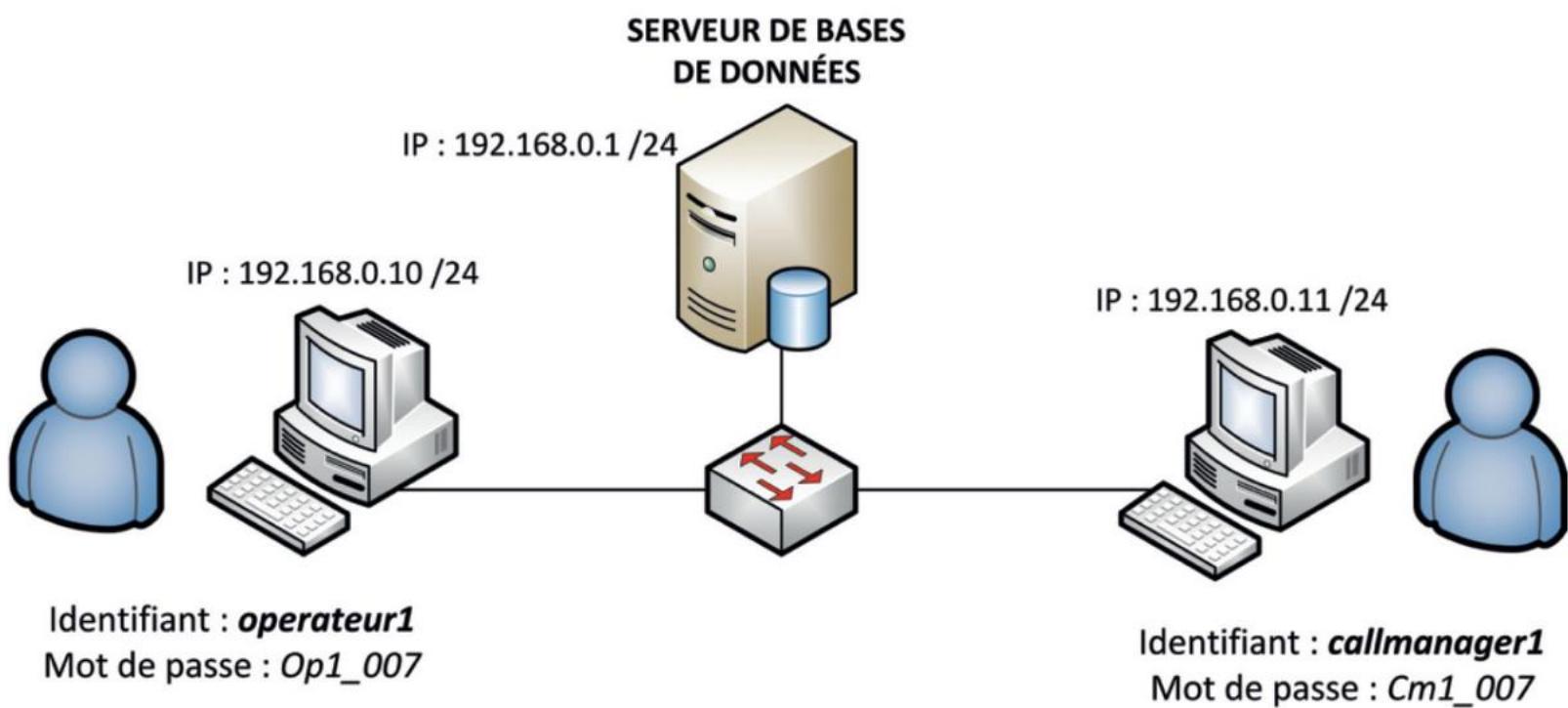
Approche démonstrative	Approche participative
<p>Le formateur transmet un message aux apprenants par une démonstration claire qui doit être, si possible, appuyée d'illustrations.</p> <p>Cette méthode peut être utilisée si le formateur a besoin de donner des informations sans avoir à soulever de problématique.</p> <p><i>Exemple : présentation par le formateur des règles à appliquer pour l'authentification des utilisateurs.</i></p>	<p>Les apprenants réalisent des travaux ou répondent à un questionnement qui va permettre de construire collectivement le message à intégrer. Cette méthode facilite la compréhension, car l'apprenant est acteur de sa formation.</p> <p><i>Exemple : un exercice guidé par des questions sur les vulnérabilités d'une application.</i></p>

Document 3 Cahier des charges de l'atelier 1 : scénario d'immersion pour la sensibilisation à la protection des données à caractère personnel

L'atelier doit attirer l'attention des stagiaires sur l'importance d'être vigilant à l'égard de la protection des données à caractère personnel et les aider à adapter leur comportement. Dans cet objectif, il a été convenu de préparer un scénario d'immersion pour la sensibilisation à la protection des données à caractère personnel.

...

•••



Paramétrage du serveur de base de données

Système d'exploitation	Debian 10
Nom de la machine	Ch2Lab1
Adresse IP	192.168.0.1 /24 (à paramétriser avec une interface en mode « pont »)
Utilisateur principal	centrecallbd
Mot de passe Utilisateur principal	centrecallbd
Super utilisateur	root
Mot de passe Super utilisateur	root
Services installés	Serveur web Apache Interpréteur PHP Serveur de bases de données Mariadb Interface de gestion : phpmyadmin

Dans le navigateur, saisir l'URL suivante : <http://192.168.0.1/phpmyadmin>.

Les identifiants et les mots de passe de connexion sont indiqués sur le schéma du réseau.

Paramétrage et tests

Importer la machine virtuelle mise à disposition, qui contient le serveur de bases de données. Un paramétrage de la carte réseau doit être conforme à la maquette présentée. Des tests de connectivité doivent être réalisés avant de commencer le scénario avec les participants.

➤ **Machine virtuelle** : www.lienmini.fr/6988-201

Mise en œuvre du scénario

- Étape 1 : connexion à la base de données de « operator1 » ; consultation de la liste des clients contenue dans la base de données ; essai de suppression de l'un d'entre eux.
- Étape 2 : connexion à la base de données de l'utilisateur « callmanager1 » ; consultation de la liste des clients contenue dans la base de données ; essai de suppression de l'un d'entre eux.
- Étape 3 : connexion de l'utilisateur « callmanager1 » à conserver pendant que l'utilisateur fait une pause ; l'« operator1 » utilise l'ordinateur de « callmanager1 » laissé libre. Il profite de la session restée ouverte pour réaliser des consultations de la table « clients ». Malheureusement, il fait une erreur de manipulation et supprime le contenu de la table. Effrayé par la gravité de son erreur et ses conséquences, il décide de ne rien dire.

➤ Voir lexique BTS SIO, p. 221

Document 4**Support de sensibilisation au respect de la confidentialité des données**

Il est décidé de sensibiliser les opérateurs téléphoniques et les *call managers* à la nécessité de ne pas laisser leur session de travail ouverte lorsqu'ils quittent leur poste. Cette affiche sera visible dans toutes les salles informatiques de l'entreprise :

Il est rappelé à l'ensemble des utilisateurs qu'il faut fermer votre session de travail avant de quitter votre poste afin de respecter la confidentialité des données.

L'équipe de la DSI

Document 5**Cahier des charges de l'atelier 2 : présentation de la politique de protection des données à caractère personnel de CentreCall**

L'atelier doit permettre de présenter la politique de protection des données à caractère personnel de CentreCall. Il comprend l'information à destination des utilisateurs du site vitrine de l'entreprise, mais aussi les éléments de la charte informatique de CentreCall. Ces informations sont inconnues des nouveaux opérateurs téléphoniques.

Document 6**Outils de présentation et d'évaluation**

Voici quelques exemples d'outils de présentation ou d'évaluation (en accès gratuit) qui peuvent être utilisés lors d'une journée de formation.

Outils de présentation	Outils d'évaluation
 Prezi Prezi est le concurrent de PowerPoint le plus connu aujourd'hui. Il permet de dynamiser les présentations avec de nombreux effets.	 Plickers est une application en ligne permettant de générer des QCM interactifs.
 LibreOffice <small>The Document Foundation</small> La solution <i>open source</i> LibreOffice propose un logiciel de présentation dont l'interface est très similaire aux anciennes versions de PowerPoint.	 Kahoot est un système de quizz en ligne, simple à utiliser et stimulant pour les participants. Il offre un état clair, sous format Excel, de ce que les apprenants ont retenu.

Fiche savoirs CEJM appliquée 2

Les données à caractère personnel : réglementation, rôle de la CNIL

Le traitement des données à caractère personnel s'inscrit dans le cadre du règlement général sur la protection des données (RGPD) de l'Union européenne. La CNIL veille à son application en France.

I

Le règlement général sur la protection des données (RGPD)

1. Les personnes concernées

Le règlement général sur la protection des données constitue le texte de référence en matière de protection des données à caractère personnel.

Il s'applique à toute organisation, publique et privée, qui traite des données personnelles de résidents de l'Union européenne.

2. Le droit des personnes

Toute personne a un droit d'accès à ses données. Elle peut les rectifier et s'opposer à leur utilisation.

Droit à la portabilité des données	Toute personne peut récupérer, sous une forme réutilisable (format lisible sur tout ordinateur), les données qu'elle a fournies à une organisation. Elle peut les transférer à un tiers.
Droit à l'oubli	Toute personne peut demander l'effacement de ses données et leur déréférencement.
Droit à la notification	En cas de violation de la sécurité des données comportant un risque élevé pour les personnes, le responsable du traitement doit avertir ces dernières rapidement. Il doit également le notifier à la CNIL dans les 72 heures.

3. Les obligations des organisations

Obligation générale de sécurité et de confidentialité	Le responsable du traitement des données doit mettre en œuvre les mesures de sécurité des locaux et des systèmes d'information et fixer une durée raisonnable de conservation des informations personnelles.
Obligation d'information	L'entreprise qui détient des données personnelles doit informer la personne concernée de : <ul style="list-style-type: none"> • l'identité du responsable du fichier; • la finalité du traitement des données; • le caractère obligatoire ou facultatif des réponses; • les droits d'accès, de rectification, d'interrogation et d'opposition; • la portabilité des données. L'objectif de la collecte d'informations doit être précis, et les données en accord avec cette finalité.
Transferts de données à l'extérieur de l'UE	Les transferts de données à l'extérieur de l'UE ne sont plus interdits, à condition d'assurer un niveau de protection suffisant (voir chapitre V du RGPD).
Délégué à la protection des données	Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au RGPD au sein de l'organisation. Il doit : <ul style="list-style-type: none"> • informer et conseiller le responsable du traitement des données et ses employés; • contrôler le respect du règlement européen et du droit français en matière de protection des données; • conseiller l'organisation sur la réalisation d'une analyse d'impact et en vérifier l'exécution.
Autres obligations	Toutes les organisations de plus de 250 salariés doivent tenir un registre des activités des traitements, sauf si ces traitements sont occasionnels.

4. La base légale des traitements des données

Le RGPD prévoit six bases légales d'application.

La sauvegarde des intérêts vitaux	Par exemple à des fins humanitaires, lorsque le traitement des données est nécessaire pour suivre des épidémies et leur propagation.
L'intérêt public	Le traitement est nécessaire à l'exécution d'une mission de service public. En cas de menace contre la sécurité publique, le DPO peut transmettre à une autorité compétente des données à caractère personnel.
Le contrat	Le traitement des données personnelles est nécessaire à l'exécution du contrat auquel les personnes ont consenti.
Le consentement	L'acceptation du traitement des données personnelles doit faire l'objet d'un consentement exprès de la personne (case à cocher, clic, etc.).
L'intérêt légitime	L'organisation a un intérêt à traiter des données qui est justifié, équilibré et ne porte pas atteinte à la vie privée.
L'obligation légale	Le traitement des données personnelles est rendu obligatoire par un texte de loi.

➤ Comprendre le RGPD : www.lienmini.fr/6988-202

➤ MOOC de la CNIL : www.lienmini.fr/6988-203

II

La CNIL

1. La mission de la CNIL

La Commission nationale de l'informatique et des libertés (CNIL) est une autorité indépendante chargée de veiller à ce que l'informatique ne porte pas atteinte aux libertés fondamentales des citoyens français.

La loi Informatique et Libertés, votée en 1978 et renforcée par la RGPD, encadre les questions liées à la protection de la vie privée en ligne. Elle définit les missions de la CNIL.

La CNIL a un rôle de conseil auprès des entreprises, des autorités publiques et du grand public. Elle fournit ainsi à l'ensemble des acteurs concernés des outils et des référentiels, pour se mettre en conformité avec le RGPD.

La CNIL est dotée d'un pouvoir de sanction renforcé avec la mise en place du RGPD : les sanctions administratives peuvent comporter des amendes jusqu'à 4 % du chiffre d'affaires mondial d'une entreprise.

2. Les cinq principes fondamentaux définis par la CNIL

Le principe de finalité	Le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime.
Le principe de proportionnalité et de pertinence	Les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier.
Le principe d'une durée de conservation limitée	Il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. La durée de conservation précise doit être fixée en fonction du type d'information enregistrée et de la finalité du fichier.
Le principe de sécurité et de confidentialité	Le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations.
Les droits des personnes	L'organisme collectant des données doit informer les individus concernés des finalités de la collecte et leur permettre d'exercer leurs droits.

➤ Voir lexique BTS SIO, p. 221

1 QCM



Retrouvez ce QCM
en version interactive
www.lienmini.fr/6988-204

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 d'une 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 traitement 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
- La loi

2

Mettre le SI en conformité avec le RGPD



> Fiche savoirs CEJMA 2



- 1 Visionnez la vidéo, puis présentez les étapes recommandées pour assurer la mise en conformité d'un SI avec le RGPD.
- 2 Expliquez en quoi la mise en conformité du SI avec le RGPD est un travail complexe.

VIDÉO

Les étapes nécessaires à la mise en conformité avec le RGPD

www.lienmini.fr/6988-205

3

Repérer les difficultés de la mise en conformité de son SI au RGPD



> Fiche savoirs CEJMA 2

Situation

Publigo est une agence de communication implantée à Louhans (Saône-et-Loire). Elle accompagne les entreprises dans la mise en place de leur stratégie digitale, en mobilisant au mieux leurs outils de communication.

Le responsable de l'agence vous communique le lien vers sa charte de confidentialité des données personnelles publiée sur son site vitrine.



- 1 Identifiez les articles de la charte répondant aux exigences légales en matière de protection des données à caractère personnel.
> Charte de confidentialité de Publigo : www.lienmini.fr/6988-206
- 2 Analysez les éléments de mise en conformité du SI avec le RGPD, et montrez que c'est un travail complexe.

4**Vérifier la conformité à la politique de protection des données personnelles**

➤ Fiche savoirs CEJMA 2

Situation

La clinique Sainte-Maure est située aux Sables-d'Olonne (Vendée), et ses bâtiments administratifs sont à la Roche-sur-Yon. Dans le cadre de son processus de recrutement, Fabien Poesman (responsable des ressources humaines) convoque les candidats pour un premier entretien et la réalisation de tests psychologiques. Vous avez pour mission de vérifier la conformité du processus de recrutement avec le RGPD, et de repérer les vulnérabilités du système d'information.

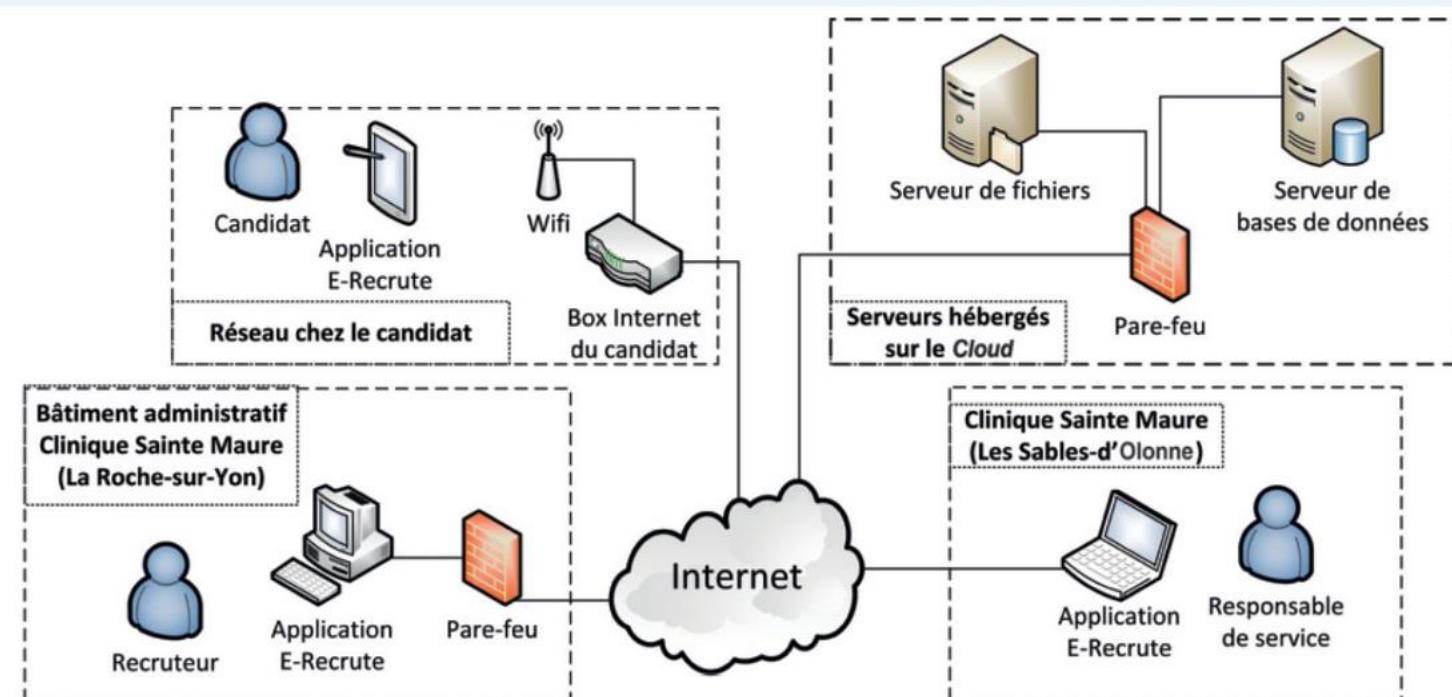
- 1** Vérifiez la conformité du processus de recrutement avec la législation sur la protection des données à caractère personnel (annexe 1).
- 2** Analysez les éléments techniques qui pourraient rendre vulnérable la protection de données personnelles (annexe 2).

Annexe 1 Processus de recrutement de la clinique Sainte-Maure

Dès l'arrivée d'un candidat, une personne de l'accueil enregistre ses données personnelles (nom, prénom, adresse, téléphone, numéro de sécurité sociale) dans l'application E-Recrute, et numérisé sa pièce d'identité. L'accès à l'application se fait grâce à un identifiant et un mot de passe, uniques pour tous les salariés de l'accueil. Il est précisé au candidat que ses données sont conservées pour une durée indéterminée afin de pouvoir le contacter ultérieurement.



Les données saisies sont enregistrées dans un serveur de bases de données, et les documents numérisés sont transférés via le protocole FTP (*File Transfer Protocol*) vers un serveur de fichiers. Les deux serveurs sont hébergés chez un prestataire sur le *cloud*. Le candidat, ainsi que les responsables des différents services de la clinique, disposent d'un identifiant et d'un mot de passe individuels pour visualiser l'ensemble des données.

Annexe 2 Extrait du schéma réseau de la clinique Sainte-Maure

5 Organiser une sensibilisation des collaborateurs à la protection des données personnelles



› Fiche savoirs CEJMA 2

- 1 Retrouvez dans cet article les éléments de sensibilisation des collaborateurs à la protection des données personnelles (annexe).
- 2 Expliquez la phrase soulignée, selon laquelle la sensibilisation des collaborateurs doit s'inscrire sur le long terme.

Annexe

La sensibilisation des collaborateurs à la sécurité informatique

Une enquête du Ponemon Institute souligne l'ampleur de la fuite des données personnelles : 76 % des informaticiens reconnaissent avoir subi une perte ou un vol de données informatiques au cours des deux années précédentes. [...]

Si certaines fuites revêtent un caractère intentionnel certain (vol de documents, de fichiers, disparition de périphériques de stockage, etc.), la majorité est simplement liée à un manque de vigilance, et peuvent donc être évitées. Sensibiliser vos collaborateurs à la sécurisation des données est incontournable pour garantir réellement la sécurité des données personnelles qui transitent dans votre entreprise. [...]

Il peut être bon de rappeler aussi que la collecte d'une donnée personnelle doit impérativement avoir une finalité précise, légale et légitime. Vous pouvez ensuite présenter des situations à risque (envoi de courriels avec diffusion d'une liste de contacts, non verrouillage de sessions, pratiques à risque lors de déplacements professionnels), puis exposer les solutions permettant d'éviter ces négligences. L'obligation de donner l'alerte en cas de fuite de données devra aussi être soulignée. [...] Vidéos, quizz, mises en situation... tout est pos-

sible ! À vous de trouver la bonne pédagogie pour capter l'attention de vos équipes et les sensibiliser à cette question. [...]

À l'appui de cette formation, il est souhaitable de constituer une documentation listant les bonnes pratiques de sécurisation des données et les questions courantes. Ces plaquettes doivent être ludiques, claires accessibles, et mises à jour en cas de besoin. Rédiger une charte informatique est aussi un très bon réflexe. [...] Afin de donner du poids à cette charte, il est possible de l'annexer au règlement intérieur de l'entreprise. Devenue ainsi obligatoire, sa violation peut alors entraîner des sanctions. Évidemment, aucune action de sensibilisation à la sécurisation des données personnelles ne peut porter ses fruits tant que l'on ne responsabilise pas les collaborateurs. Il est possible d'inclure des clauses de confidentialité spécifiques dans les contrats de travail (cette clause de confidentialité porte alors spécifiquement sur les données personnelles). In fine, la sensibilisation de ses collaborateurs à la sécurité des données doit s'inscrire sur du long terme.

« Comment organiser la sensibilisation rgpd de vos collaborateurs ? », print-value.fr



Évaluation 1

L'organisation cliente

Créé en 1986, le groupe Terre&Mer85 compte aujourd'hui 15 agences situées sur l'ensemble de la côte atlantique. Son activité principale est l'organisation de séjours sur le littoral. Le groupe compte 50 collaborateurs dont 6 sont au siège social situé à La-Roche-sur-Yon dans la zone industrielle Nord.

Le réseau informatique est géré par la DSI du groupe mais elle délègue à des prestataires certaines opérations spécifiques, comme des audits de sécurité de leur système d'information.

La DSI de Terre&Mer85 a récemment été alertée de la violation de données à caractère personnel lors du traitement des inscriptions des nouveaux clients en agence.

Le groupe Terre&Mer85 fait appel à la société Audit44, spécialisée dans l'audit des systèmes d'information, afin d'identifier les vulnérabilités du traitement des inscriptions et proposer des solutions adaptées.

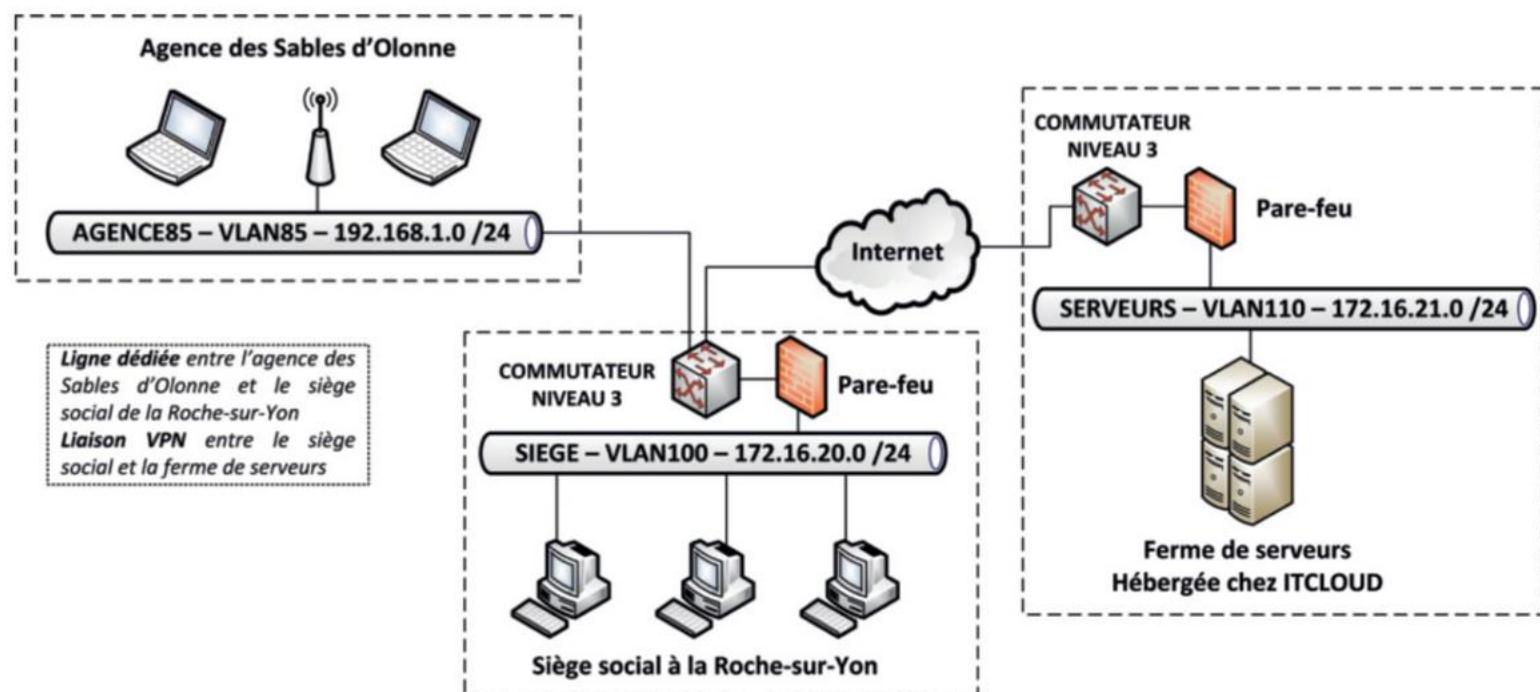


Le prestataire informatique

La société Audit44, située à Nantes, est spécialisée dans l'audit et l'accompagnement des entreprises pour améliorer le processus de leur système d'information.

En tant que nouveau salarié de cette société, vous devez prendre en charge l'audit du traitement des inscriptions des nouveaux clients.

Architecture réseau du groupe TERRE&MER85



Votre mission

Votre mission consiste, dans un premier temps, à participer au recensement des vulnérabilités dans le processus de traitement des inscriptions. Dans un second temps, vous proposez des solutions adaptées pour assurer la mise en conformité avec la législation des traitements réalisés sur les données à caractère personnel. Vous vous appuyez sur le dossier documentaire mis à votre disposition.

Missions

1 Analyser les risques sur les traitements des données à caractère personnel

Dans cette première mission, vous devez diagnostiquer les vulnérabilités et le niveau de risque sur les données à caractère personnel lors des inscriptions en agence. Pour cela, vous disposez d'un entretien avec la responsable d'agence des Sables-d'Olonne et de divers documents fournis par la DSI du groupe.

- 1.1.** Repérez les vulnérabilités organisationnelles et technologiques sur la protection des données à caractère personnel.
- 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.
- 1.3.** Commentez le niveau de risque diagnostiqué pour le traitement des inscriptions.

2 Mettre en conformité le traitement des inscriptions des clients avec la législation

Dans cette deuxième mission, vous devez vérifier la conformité avec la législation de la protection des données à caractère personnel, notamment la conformité des conditions d'hébergement des serveurs par la société ITCloud, spécialisée dans la location de serveurs virtuels accessibles via une connexion Internet.

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

Dossier documentaire

Document 1

Entretien avec la responsable d'agence des Sables-d'Olonne

Vous : Bonjour M^{me} Letot, je travaille pour la société Audit44. Comme convenu avec la direction de votre groupe, j'aimerais vous interroger sur les traitements réalisés lors de l'inscription de vos clients. Pouvez-vous me résumer le processus d'inscription d'un nouveau client de Terre&Mer85 ?

M^{me} LETOT : Bonjour. Lors du premier contact avec un nouveau client, nos collaborateurs en agence saisissent les informations personnelles et rédigent son profil, en rapport avec les résultats de l'entretien. Un profil peut être par exemple : « personne retraitée disponible et disposant d'un budget conséquent ».

Vous : Si je comprends bien, l'ensemble de ces informations est transmis et stocké directement sur les serveurs distants du groupe ?

M^{me} LETOT : Non, pas directement. En tant que responsable d'agence, je suis la seule habilitée à valider la correspondance du profil établi avec l'ensemble



des données collectées. Je peux parfois apporter des changements avant de valider une insertion dans la base de données distante. Cependant, il m'arrive de communiquer mes codes d'accès à un collaborateur de confiance afin qu'il réalise cette action en mon absence.

Document 2 Privilèges des collaborateurs de l'agence des Sables-d'Olonne sur la base de données Terre&Mer85

Nom d'utilisateur	Nom d'hôte	Privilèges	Grant
Manageur85100	%	SELECT, INSERT, UPDATE, DELETE	Non
Operateur1	%	SELECT	Non
[...]	[...]	[...]	[...]
Root	%, localhost	ALL PRIVILEGES	Oui

% : tous les hôtes.

Document 3

Note interne pour les transferts de documents numérisés

Les documents numérisés lors de la création d'un compte client (comme le passeport par exemple) doivent être transférés sur le serveur de fichiers via le protocole FTP (*File Transfer Protocol*). Pour cela, vous avez à votre disposition l'application TransDoc, créée par notre service de développement de solutions logicielles.

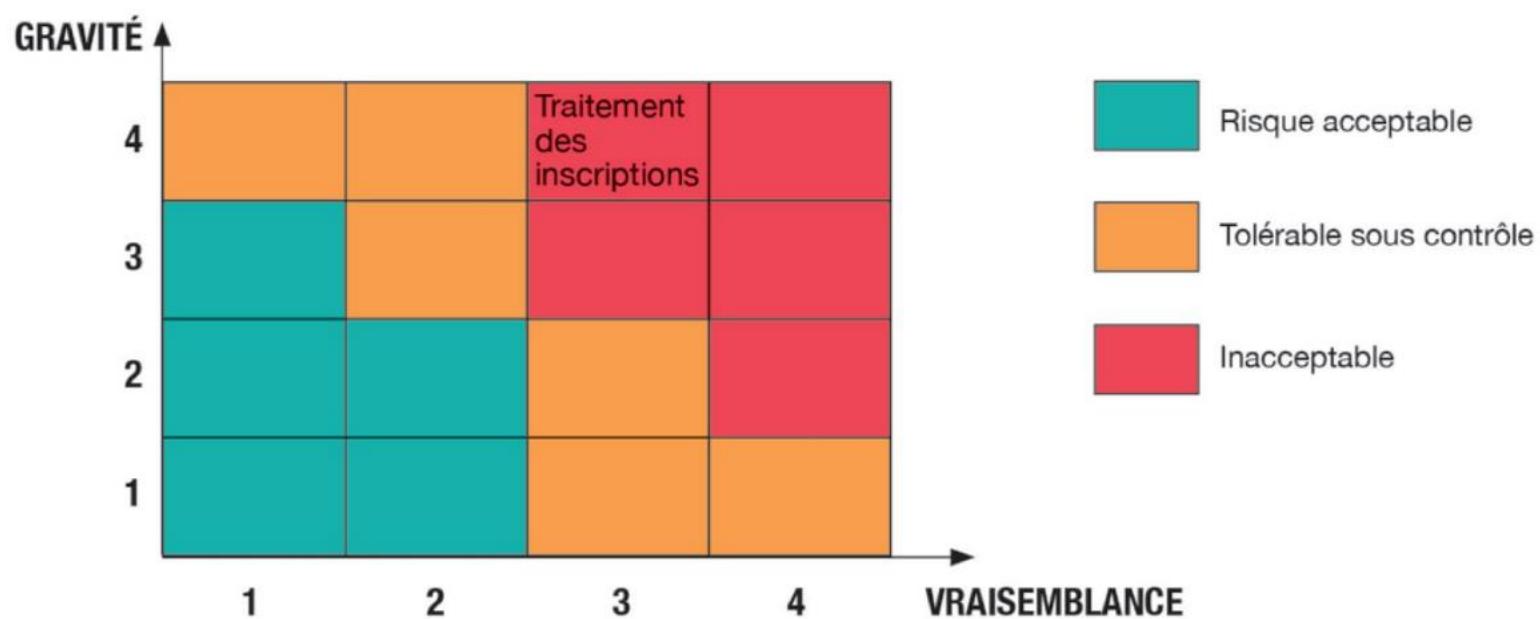
L'identifiant et le mot de passe à utiliser sont les mêmes que ceux qui donnent accès à la base de données.

Le service DSI du groupe Terre&Mer85

Document 4

Cartographie des risques sur le traitement des données lors des inscriptions des nouveaux clients

La cartographie présentée est le résultat de l'utilisation de la méthode EBIOS Risk Manager (expression des besoins et identification des objectifs de sécurité), développée par l'ANSSI.



Document 5

Les engagements d'ITCloud concernant la sous-traitance du traitement des données personnelles

→ Engagement n° 1 : la non-réutilisation des données hébergées sur nos services

Les informations hébergées dans le cadre de nos services restent la propriété du client. Nous nous interdisons toute revente desdites données, de même que toute utilisation à des fins commerciales (telles des activités de profilage ou de marketing direct).

→ Engagement n° 2 : permettre la réversibilité de vos données

Chez ITCloud, 100 % de nos solutions de *cloud* sont basées sur des standards, dont un certain nombre de technologies *open source*. Vous pouvez donc récupérer vos données facilement : la réversibilité et l'interopérabilité sont toujours possibles.

→ Engagement n° 3 : savoir précisément où sont stockées et traitées vos données

Plusieurs localisations ou zones géographiques sont disponibles, vous pouvez opter pour celle de votre choix au moment de la commande.

Lorsque vous sélectionnez une zone de stockage située dans l'Union européenne, ITCloud vous garantit qu'il ne traite pas vos informations en dehors

de l'Union européenne ou de tout pays reconnu par la Commission européenne comme disposant d'un niveau de protection des données à caractère personnel suffisant. De plus, nous nous engageons à ne jamais traiter vos données aux États-Unis.

→ Engagement n° 4 : vous informer en cas de violation de données

Dans l'éventualité d'une violation d'informations, nous nous engageons à informer les clients concernés dans les meilleurs délais. Cette notification précisera la nature de l'incident, ses conséquences prévisibles, ainsi que les mesures prises pour résoudre ou minimiser la violation.

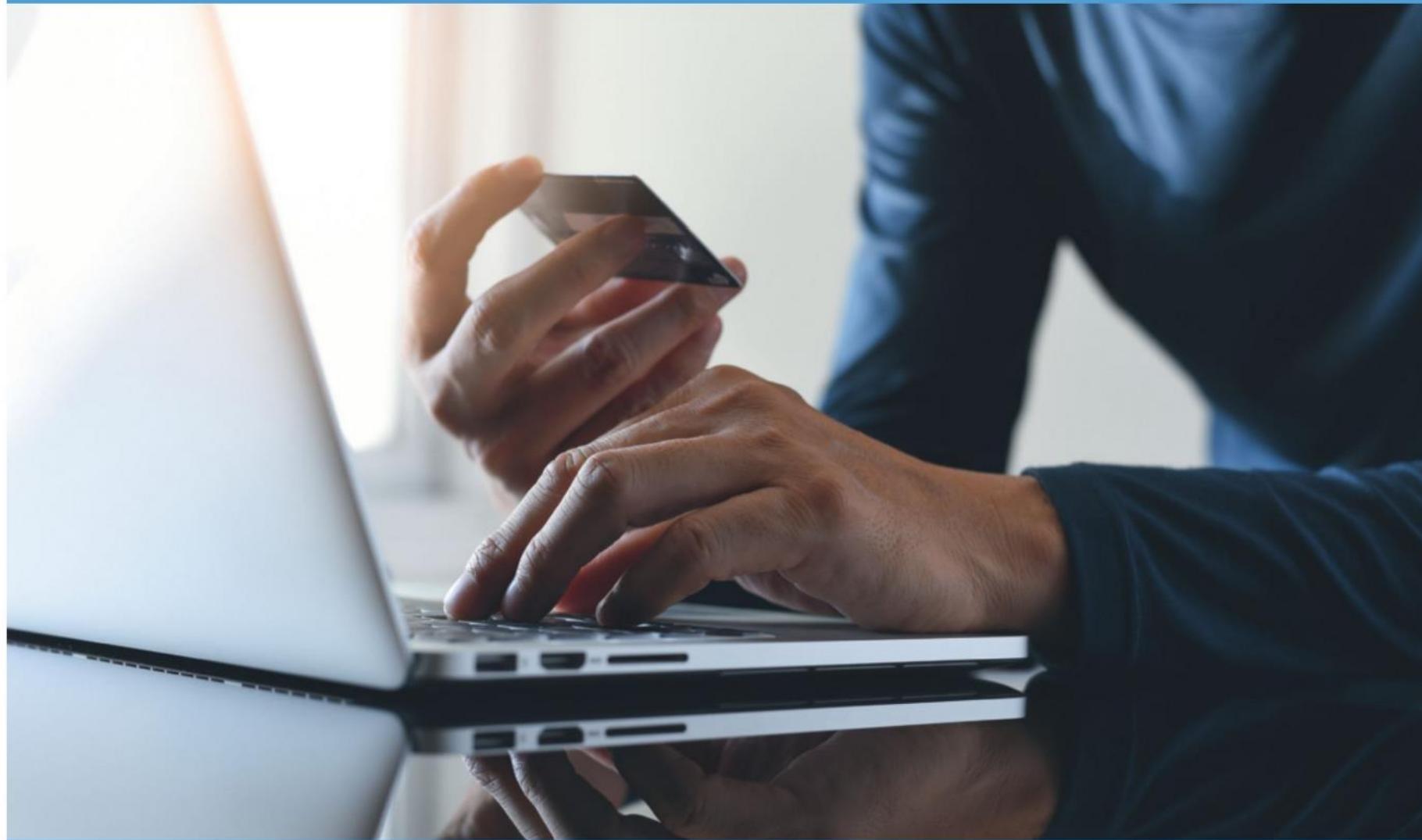
Il est essentiel de faire la distinction entre la sécurité des données hébergées par le client et la sécurité des infrastructures sur lesquelles ces informations sont stockées.

- Sécurité des données hébergées : le client est seul responsable de la sécurisation des ressources et des systèmes applicatifs qu'il déploie, dans le cadre de l'utilisation de nos services.
- Sécurité des infrastructures : ITCloud s'engage à sécuriser ses infrastructures de façon optimale.



Contexte 2

Préserver l'identité numérique de l'organisation



L'organisation cliente

M@Banque est une néobanque fondée en 2018 sur le modèle de banques en ligne comme Orange Bank, N26 ou Revolut, les leaders actuels du marché.

Moins chère que les banques physiques, une néobanque offre des services plus restreints mais ciblés, tels que l'ouverture sans délai d'un compte courant, ou encore des outils innovants de gestion des transactions financières (retrait, virement, dépôt), exclusivement sur l'application mobile.

La législation a favorisé l'essor des néobanques en obligeant les banques à faciliter la mobilité bancaire. Leur activité purement digitale les amène à porter une attention toute particulière à la protection de leur identité numérique.

VIDÉO

Caractéristiques et avantages d'une néobanque



www.lienmini.fr/6988/2001

Le prestataire informatique

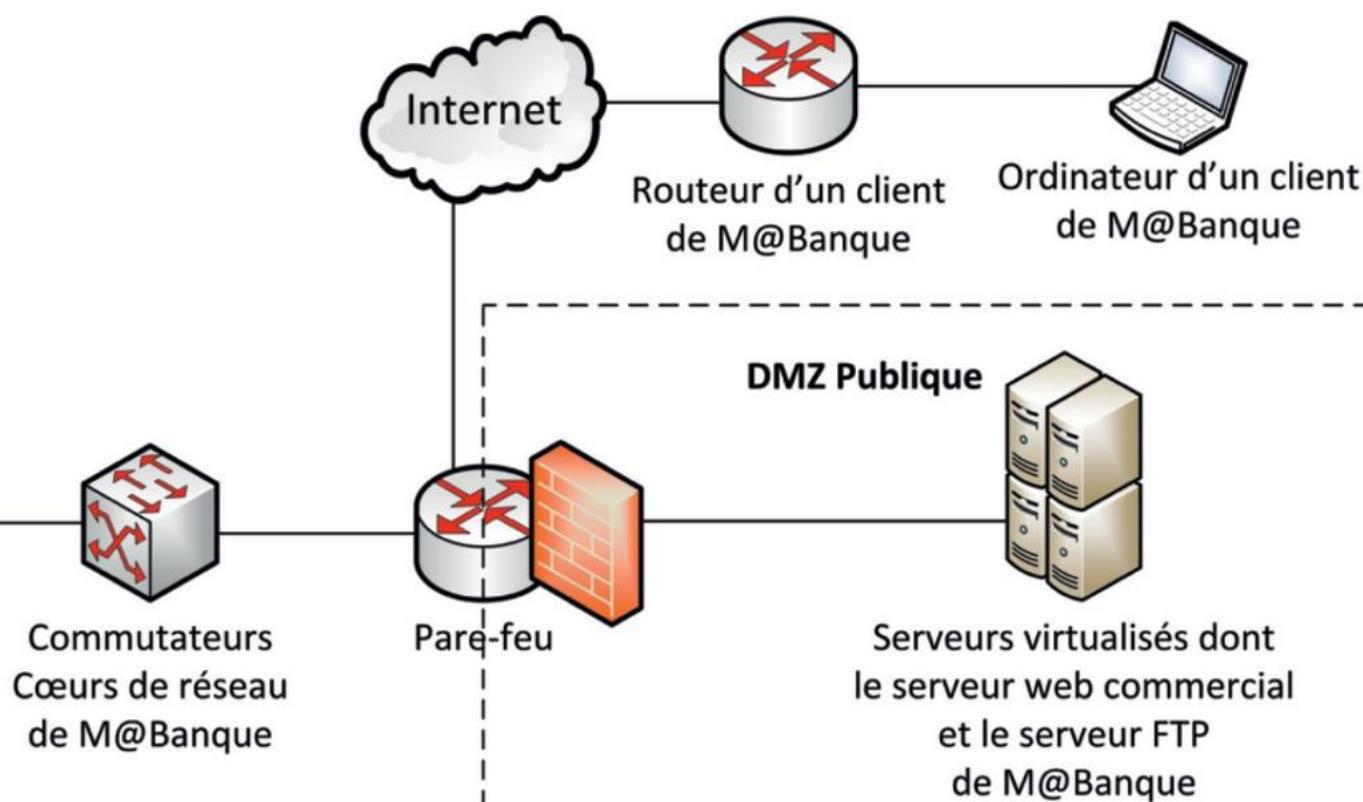
La DSI de M@Banque, implantée à Strasbourg, compte 20 collaborateurs. Dirigée par M. Legros, elle compte un pôle dédié à la protection de l'identité numérique de la société. Ce pôle est constitué de quatre salariés à temps plein, en relation constante avec M^{me} Schmitt, *community manager* de M@Banque. Cette dernière a notamment pour mission de gérer la communication

de M@Banque sur les différents réseaux sociaux et sur le site vitrine de l'entreprise. Formée au droit de la preuve électronique et à la protection de l'identité numérique des organisations, elle veille au respect de la législation. En cas d'atteintes extérieures, elle contribue à la conception de solutions techniques avec le pôle dédié.

Contexte 2

Description du SI de l'organisation

Schéma général du réseau de M@banque



Cahier des charges

Deux récentes cyberattaques – la défiguration du site commercial et une tentative d'hameçonnage des courriels – ont fait apparaître les vulnérabilités du système d'information de ma M@Banque et inquiètent les clients.

À la suite de la défiguration qui a modifié l'apparence du site, la DSI a pour objectif de rétablir la e-réputation

de M@Banque. Elle souhaite déployer les moyens techniques et juridiques appropriés : mise en place de solutions techniques permettant de protéger l'identité numérique de M@Banque, supports appropriés de preuves électroniques.

Cette mission nécessite l'association de compétences techniques et juridiques.

Votre mission

Vous êtes nouvellement recruté(e) dans le pôle Protection de l'identité numérique de la DSI de M@Banque. Votre bureau est situé près de celui de M^{me} Schmitt, *community manager*. Ensemble, vous mettez en place des solutions techniques permettant de protéger l'identité numérique de M@Banque.

Préserver l'identité numérique de l'organisation

COMPÉTENCES

- Protéger l'identité numérique d'une organisation
- Déployer les moyens appropriés de preuve électronique

SAVOIRS ASSOCIÉS

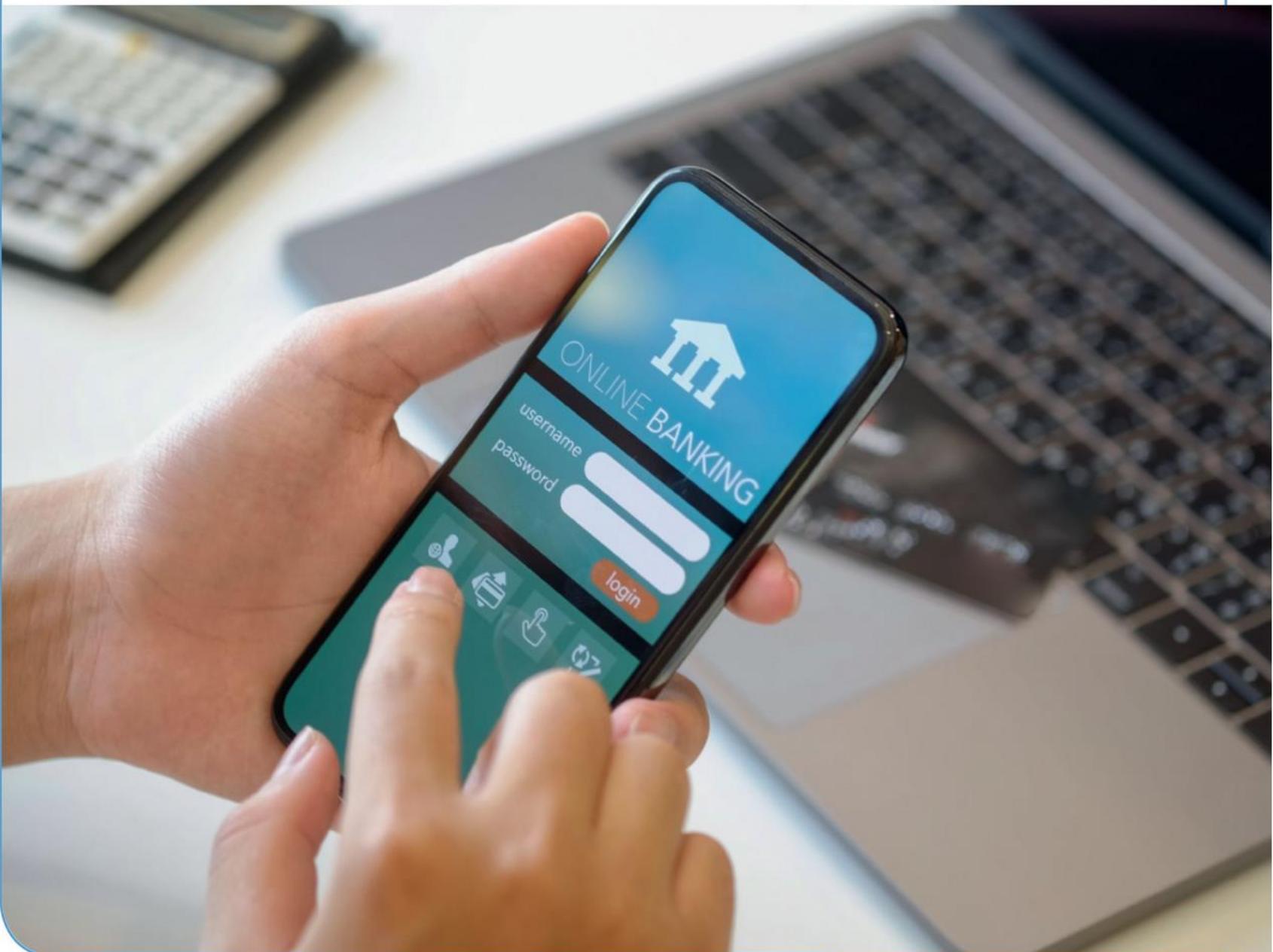
- L'identité numérique de l'organisation : risques et protection juridique
- Droit de la preuve électronique
- Les risques des cyberattaques pour l'organisation : économique, juridique, atteinte à l'identité de l'entreprise

Situation professionnelle

Pour les clients d'une néobanque comme M@Banque, qui n'ont pour interlocuteurs que des interfaces numériques, la confiance dans la sécurité informatique est primordiale.

Deux événements majeurs ont mis à mal la sécurité du système informatique de M@Banque : la **défiguration** par des hackers du site commercial de la société et la réception par les clients de courriels frauduleux au nom de la société. Le *community manager* de

M@Banque vous informe que de nombreux messages sur les réseaux sociaux relaient ces récents événements en dénonçant la faiblesse de la sécurité informatique de la société. Ils contribuent ainsi à en détériorer l'e-réputation. Vous êtes chargé(e) de faire le diagnostic de la situation pour chacun des événements (*hacking* et courriels frauduleux) afin de trouver des solutions technologiques pour améliorer la protection de l'**identité numérique** de M@Banque et rétablir la confiance de ses clients.



➤ Voir présentation générale, p. 55

Missions professionnelles

1

Protéger l'identité numérique de l'organisation



M^{me} Schmitt, *community manager*, vient de vous alerter de la défiguration du site commercial de M@Banque.

L'identité numérique de l'entreprise est directement attaquée. Les données personnelles des clients ont été piratées. Dans un secteur fortement concurrentiel, M@Banque doit démontrer qu'elle peut protéger les avoirs bancaires de ses clients et en sécuriser les accès. M^{me} Schmitt vous demande d'identifier les **vulnérabilités** qui ont permis cette cyber-attaque afin de proposer des solutions techniques adaptées.

Travail à faire

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

➤ Document 1
➤ Fiche savoirs CEJMA 3

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.

➤ Fiches savoirs CEJMA 3 et 5

Les scripts du site commercial de M@Banque sont régulièrement mis à jour par un seul développeur, uniquement depuis son poste de travail dédié (adresse IP : 172.16.8.10/16). Il utilise le logiciel Filezilla, qui permet de transférer les fichiers à un serveur via le protocole FTP.

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

➤ Documents 2 et 3

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

➤ Document 4

Les hackers du site de M@Banque ne se sont pas contentés de commettre cet acte de malveillance. Ils ont également diffusé de mauvaises appréciations sur les réseaux sociaux, ce qui a amené de nombreux clients à envoyer des courriels pour exprimer leurs inquiétudes.

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.

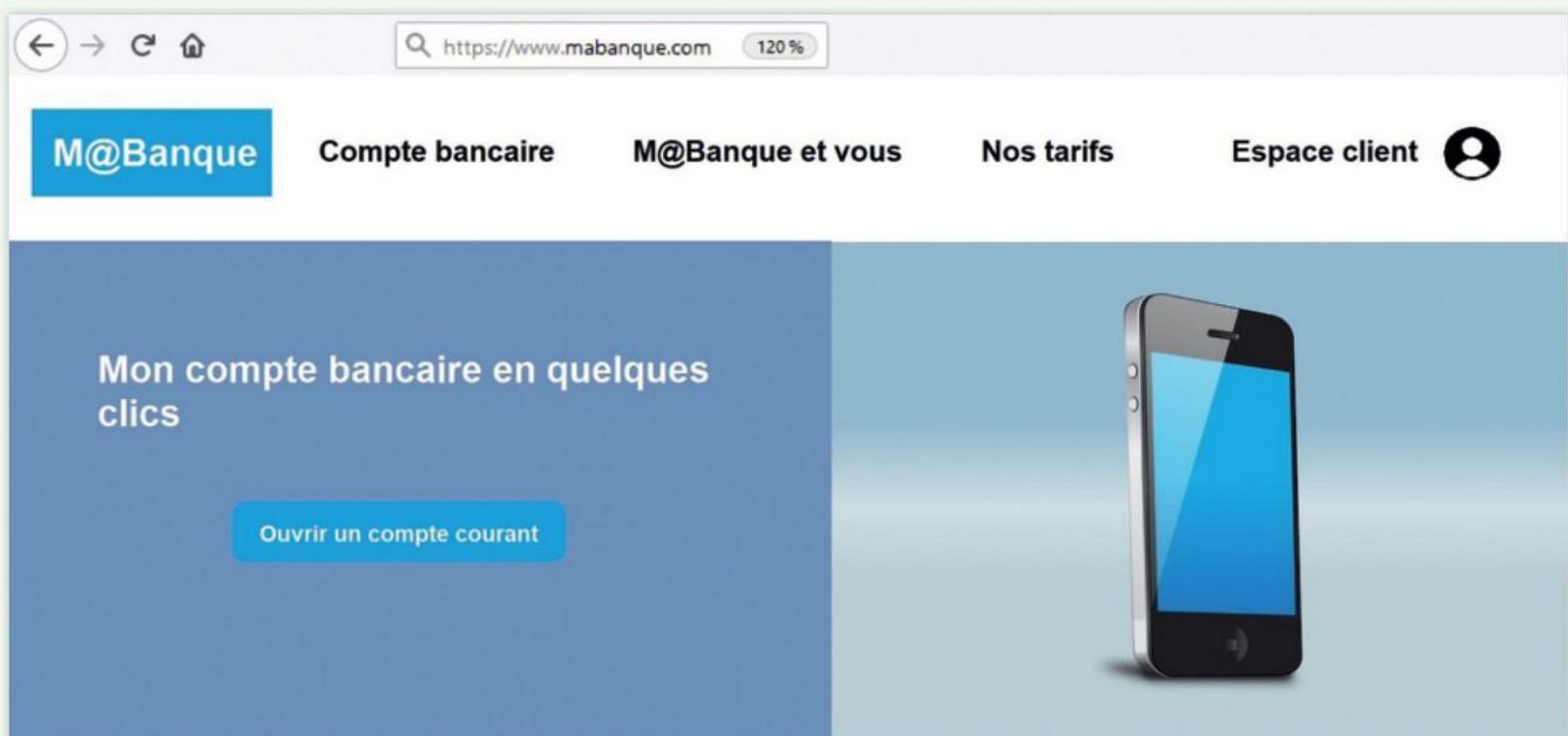
➤ Document 5
➤ Fiches savoirs CEJMA 3 et 5

➤ Voir lexique BTS SIO, p. 221

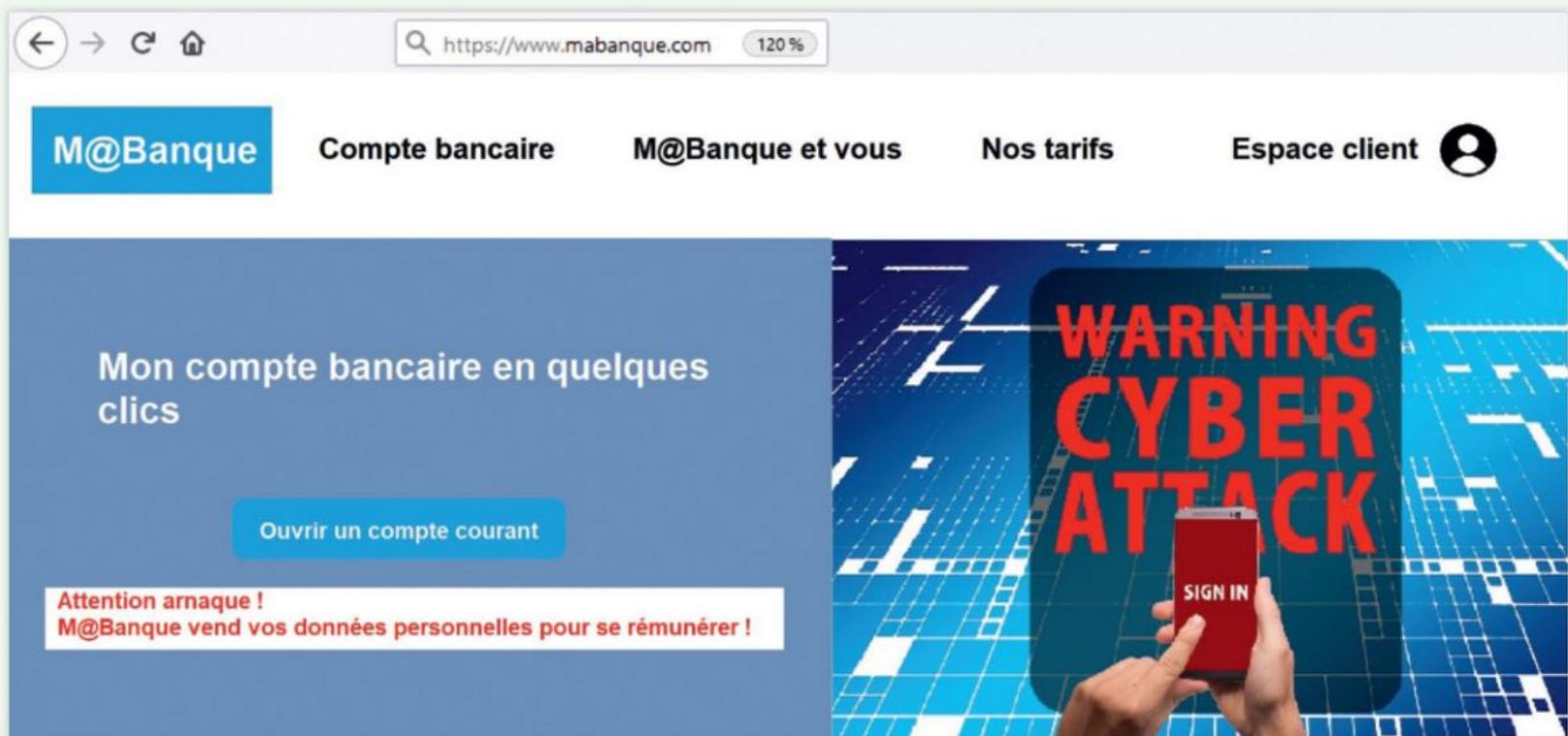
Dossier documentaire

Document 1 Le site défiguré de M@Banque

L'apparence du site avant sa défiguration



L'apparence du site après sa défiguration

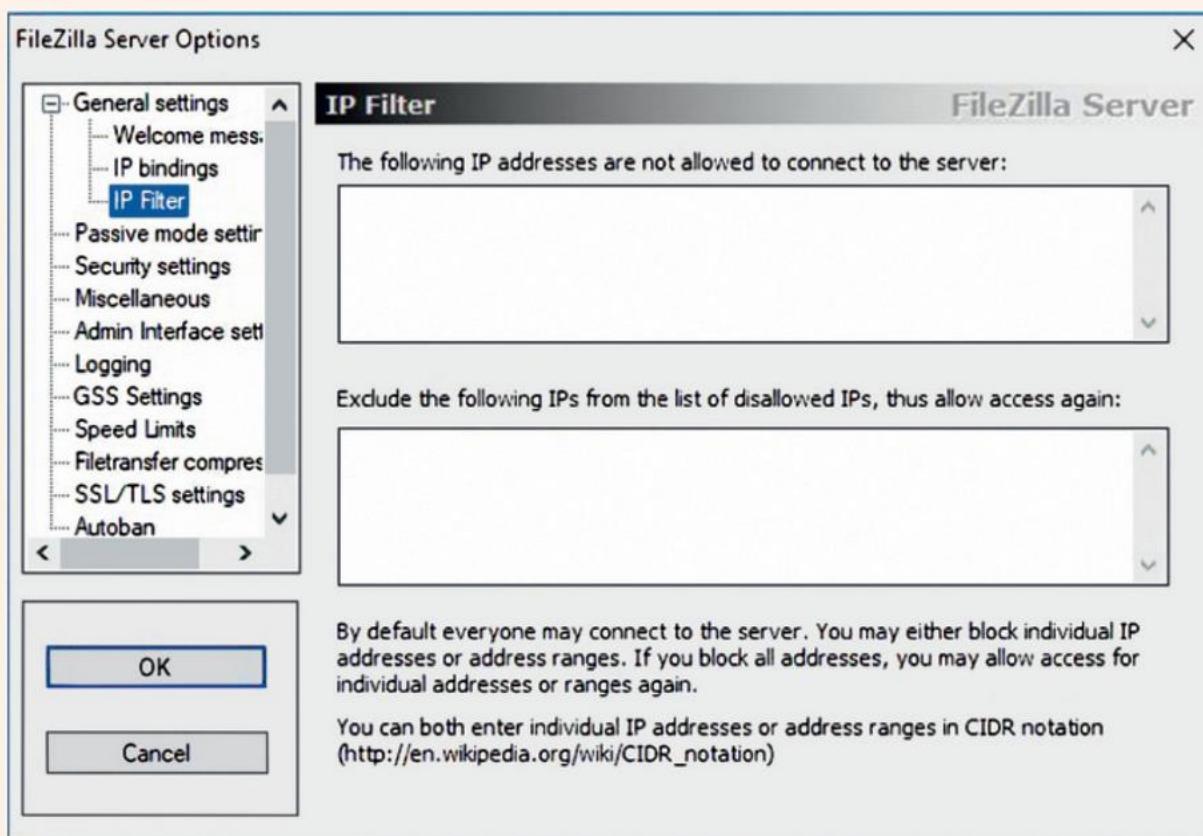


Document 2 Extrait du fichier log du serveur FTP

```
(000005) 17/01/2020 13:52:56 - (not logged in) (172.16.56.20)> AUTH TLS
(000005) 17/01/2020 13:52:57 - (not logged in) (172.16.56.20)> 234 Using authentication type TLS
(000005) 17/01/2020 13:52:57 - (not logged in) (172.16.56.20)> SSL connection established
(000005) 17/01/2020 13:53:04 - (not logged in) (172.16.56.20)> USER admiweb
(000005) 17/01/2020 13:53:04 - (not logged in) (172.16.56.20)> 331 Password required for admiweb
(000005) 17/01/2020 13:53:04 - (not logged in) (172.16.56.20)> PASS *****
(000005) 17/01/2020 13:53:04 - pilote (172.16.56.20)> 230 Logged on
```

Missions professionnelles

Document 3 L'interface de configuration du serveur FTP



Document 4 La veille sur la restriction d'accès à l'interface de gestion

Qu'il s'agisse d'une interface incluse dans le site Web permettant de modifier dynamiquement son contenu, ou d'un accès direct aux fichiers du site (par FTP, SSH, RDP, etc.), le CERT-FR recommande de mettre en place une politique de gestion des autorisations d'accès. Cela peut passer par la mise en place d'une liste blanche réduite d'adresses IP depuis lesquelles des administrateurs ou des contributeurs peuvent légitimement effectuer des modifications. La validation des accès par rapport

à cette liste blanche est appliquée par la configuration du service d'administration (FTP, SSH, RDP, etc.), ou la mise en place de fichiers *.htaccess* pour limiter l'accès à des répertoires particuliers. Dans le cas où les adresses IP des administrateurs ne sont pas statiques, une authentification forte (validation de certificats clients, par exemple) doit être envisagée.

www.cert.ssi.gouv.fr

Document 5 Le message sur le compte Twitter de M@Banque

M@Banque a été victime d'une rumeur négative (*bad buzz*) lorsque les clients ont constaté la défiguration de son site commercial.

Les messages postés sur Twitter à propos de M@Banque peuvent être préjudiciables pour l'entreprise.

Missions professionnelles

2

Déployer les moyens appropriés de preuves électroniques

Des courriels frauduleux sont adressés aux clients, qui prennent l'apparence de messages émis par M@Banque. Ils les invitent à compléter un contrat dématérialisé d'ouverture de compte avec leurs informations personnelles. Si les clients remplissent le document, les pirates peuvent récupérer leurs informations d'identification pour accéder à leurs comptes. Mme Schmitt sollicite votre expertise pour trouver une solution technique à cet acte de malveillance et rétablir l'e-réputation de M@Banque.



Travail à faire

1. Identifiez les éléments permettant de détecter que le courriel contenant un contrat dématérialisé est frauduleux.
 - Documents 1 et 2
 - Fiche savoirs CEJMA 4
2. Déterminez le délit et les peines encourues par les pirates pour cet acte de malveillance.
 - Fiche savoirs CEJMA 3

Un client a adressé un courriel à M@Banque pour confirmer la signature d'un contrat de demande de carte de crédit en utilisant une solution de chiffrement (document 4). Votre responsable s'interroge sur la valeur de ce document en cas de litige.

3. Démontrez que la solution proposée pour les échanges de contrats dématérialisés répond bien aux exigences de la législation.
 - Documents 3 et 4
 - Fiche savoirs CEJMA 4

M@Banque souhaite proposer à ses clients la mise à disposition d'un coffre-fort numérique pour protéger leurs documents numériques.

4. Présentez les avantages d'une telle solution pour les clients et pour le rétablissement de l'e-réputation de M@Banque.
 - Document 5
 - Fiche savoirs CEJMA 4

Missions professionnelles

Dossier documentaire

Document 1 Le courriel reçu par les clients de M@Banque

M@Banque

Cher(e)s clients et clientes de M@Banque

Vous trouverez en pièce-jointe le contrat d'ouverture de compte bancaire à compléter et à nous renvoyer pour confirmer votre engagement pris via notre site.

Vous devrez nous confirmer notamment votre identifiant et votre mot de passe d'accès à vos comptes.

Nous sommes heureux de vous compter parmi nos nouveaux clients.

Le service juridique

servicejuridique@mabanques.com

Document 2 Le rappel des conseils de la CNIL figurant sur le site M@Banque

1. Généralement, les messages malveillants sont envoyés à destination d'un grand nombre de cibles, ils ne sont pas ou peu personnalisés.
 2. Le message évoque un dossier, une facture, un thème qui ne vous parle pas ? Il s'agit certainement d'un courriel malveillant.
- **Attention aux expéditeurs inconnus :** soyez particulièrement vigilants sur les courriels provenant d'une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.
 - **Soyez attentif au niveau de langage du courriel :** même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration...).
 - **Vérifiez les liens dans le courriel :** avant de cliquer sur les éventuels liens, laissez votre souris dessus. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime.
 - **Méfiez-vous des demandes étranges :** posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.
 - **L'adresse de messagerie source n'est pas un critère fiable :** une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique.

Extrait de « Phishing : détecter un message malveillant », www.cnil.fr.

➤ Voir lexique BTS SIO, p. 221

Document 3 Les indications de la direction de M@Banque concernant la gestion des contrats dématérialisés

La direction de la banque a envoyé une note aux employés chargés de la gestion des contrats dématérialisés afin de leur rappeler les règles essentielles à respecter.

M@Banque

Il est rappelé à tous les collaborateurs qu'il est possible pour les particuliers de souscrire un contrat dématérialisé si les deux règles suivantes sont respectées :

- l'authentification claire des signataires du contrat ;
- l'intégrité du document.

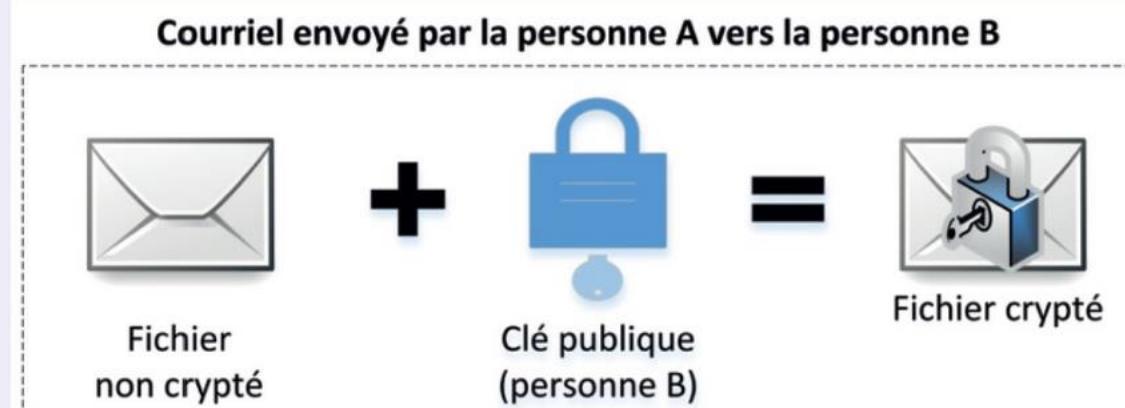
Si ces conditions sont respectées, alors le contrat numérique équivaut à un contrat papier aux yeux de la loi : ils ont donc la même valeur légale.

Vous pouvez ainsi recommander aux clients qui le souhaitent d'utiliser un logiciel de signature électronique (par exemple, GnuPG) et un coffre-fort électronique pour la création, la signature et l'archivage de documents contractuels.

Cordialement,
La Direction M@Banque

Document 4 Une veille pour une solution de cryptage de courriels

Le principe de PGP (*Pretty Good Privacy*) repose sur une cryptographie à clé publique. C'est-à-dire qu'une paire de clés publiques et une paire de clés secrètes sont générées. La clé secrète (*key*) est protégée par un mot de passe et sert à déchiffrer. Elle reste sur l'ordinateur de son propriétaire, tandis que la clé publique sert à chiffrer ses emails et est distribuée au plus grand nombre. Ainsi, la clé publique est mise à disposition des contacts email potentiels, en leur étant distribuée directement ou encore en la téléchargeant via un serveur de clés externe. À l'aide de la clé publique, il est possible de crypter tous les emails que l'on échange avec vous. La clé privée est uniquement en votre possession, et protégée de surcroît par un mot de passe. Pour que vous puissiez communiquer en toute sécurité, il est nécessaire que votre contact utilise également PGP et partage la clé publique avec vous. Le procédé de la clé publique est également désigné comme étant un processus asymétrique, car les deux parties utilisent des clés différentes. À l'aide de signatures, vous pourrez d'autant plus garantir l'authenticité de vos communications.



Missions professionnelles

Document 5 La solution du coffre-fort numérique de M@Banque

Le coffre-fort numérique proposé par M@Banque est une solution de stockage d'informations certifiée sans intrusion possible. Son objectif est de conserver les données intactes et de permettre leur restitution à l'identique à un utilisateur accrédité. Le coffre-fort numérique doit donc garantir, avant tout, l'intégrité des informations dans le temps.

Ce service est désormais proposé aux particuliers, sous la forme d'un espace de stockage sécurisé, qui nécessite une identification. Ses fonctionnalités permettent la récupération automatique des différents types de documents confiés par le client (relevés bancaires, fiches de paie, factures, diplômes, papiers d'identité, documents administratifs ou fiscaux, etc.). Une fois configuré, cet outil aspire donc automatiquement les nouveaux documents produits par M@Banque (par exemple, un relevé de compte bancaire).

M@Banque garantit, à l'utilisateur, un « accès exclusif » du service par la mise en œuvre des mesures suivantes :

- une identification par un identifiant et un mot de passe personnels ;
- un chiffrement par le service de coffre-fort numérique de l'ensemble des documents et données lors de leurs stockages, transferts vers ou depuis le service.

The screenshot shows a web browser window with the URL <https://www.mabanque.com> in the address bar. The page title is "Coffre-fort numérique". On the left, there is a blue header bar with the "M@Banque" logo. The main content area has a blue background. It features a placeholder text box for "Identifiant client" (client identifier) and a lock icon. Below it is a placeholder text box for "Mot de passe" (password). To the right of the password field is a "Valider" (Validate) button. At the bottom left, there is a 3x3 grid of numbers: 9, 2, 5 in the top row; 4, 7, 1 in the middle row; and 6, 3, 8 in the bottom row.

1

Protéger l'identité numérique de M@Banque



La défiguration du site de M@Banque a montré la nécessité d'informer les clients sur les moyens de vérification de l'intégrité d'un site Web pour éviter que leurs outils numériques (smartphones, ordinateurs, tablettes, etc.) ne soient infectés. Cette action doit apporter une contre-mesure utile pour rétablir la confiance des clients en démontrant la capacité de M@Banque à protéger son identité numérique. Votre mission est de tester et réaliser un comparatif de solutions permettant l'audit du site Web de M@Banque.

Pour ce travail, vous allez prendre pour exemple le site de votre concurrent direct : www.n26.com

1. Complétez le tableau d'organisation de la veille technologique.
➤ Document 1
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.
➤ Document 2
➤ Fiches méthode 1 et 2, pp. 203 et 205
3. Retrouvez au moins deux autres outils d'audits de sécurité de sites Web à l'aide des résultats de vos recherches.
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.
➤ Documents 3 et 4
5. Rédigez 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.

Document 1 La qualité et la pertinence des informations collectées

Objectifs de la veille technologique						
Sources d'informations	Créabilité de l'auteur	Fiabilité de la source	Objectivité de l'information	Exactitude de l'information	Actualité de l'information	Pertinence de l'information
Exemple : site Web...						
Évaluation						

Chaque critère d'évaluation de la qualité des sources d'information sera noté de 1 à 4 (1 étant la note indiquant que le critère n'est pas du tout respecté).

Document 2 Les outils de collecte, traitement, curation et partage de l'information

	Outil de collecte de l'information	Outil de traitement de l'information	Outil de curation de l'information	Outil de partage des résultats
Nom de l'outil				
Avantages				
Inconvénients				

Document 3 Tester en ligne la sécurité d'un site Web

Le test de sécurité permet de s'assurer qu'un site n'est pas infecté par un *malware*, victime d'une défiguration, blacklisté ou encore utilisé pour spammer. L'attaque d'un site devient visible et problématique quand :

- une marque concurrente informe l'entreprise que son site est utilisé pour vendre illégalement des produits ;
- quand le site se met à dysfonctionner.

Il existe de nombreux outils en ligne gratuits pour tester et vérifier l'intégrité d'un site Web. Ces outils ne mesurent pas l'intégrité des sites selon les mêmes critères et sont plus ou moins performants. Il existe, par exemple :

- le Google Safe Browsing (<https://transparencyreport.google.com/safe-browsing/search>) ;
- le URLVoid (<https://www.urlvoid.com/>).

Document 4 Un tableau comparatif des outils d'audits de sécurité de site Web

Critères d'analyse	Google Safe Browsing	URLVoid
<i>Malware</i>		
<i>Spam</i>		
...		

Travaux en laboratoire informatique

2

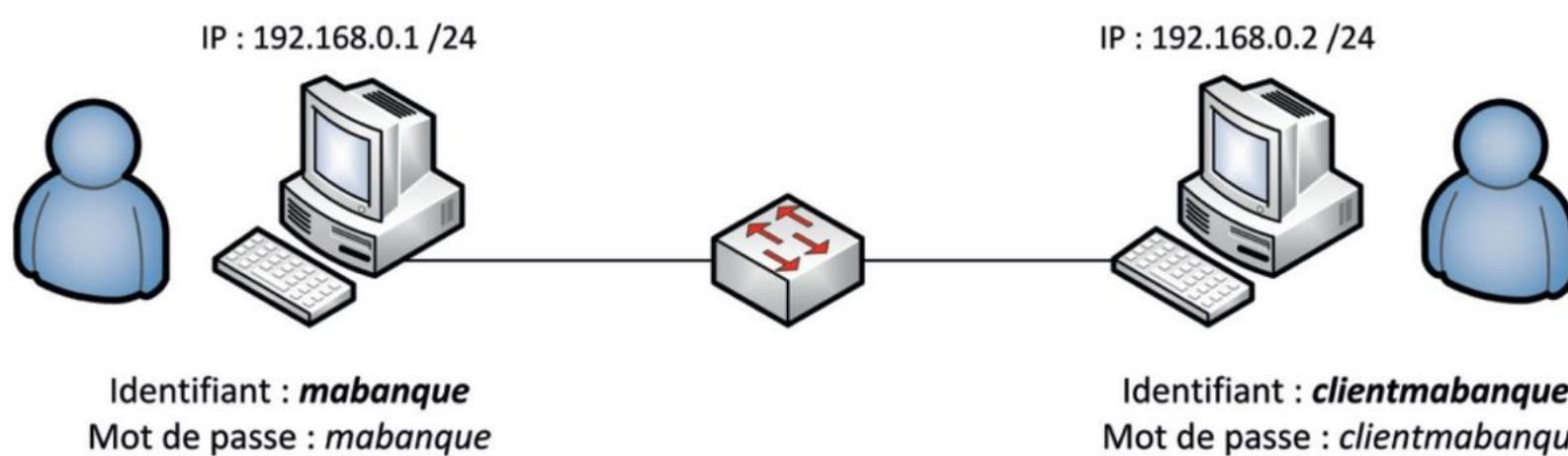
Déployer des moyens de preuves sécurisés et conformes à la législation



Lors de votre mission précédente, vous avez réalisé une veille sur les technologies qui permettent de crypter les contenus de courriels PGP. Votre responsable vous demande maintenant de mettre en œuvre cette technologie dans un environnement prototypé. Les conclusions de vos analyses permettront de renforcer les moyens de preuves sécurisés.

1. Importez les deux machines virtuelles dans votre logiciel de virtualisation (par exemple, VirtualBox) afin d'obtenir l'environnement de test.
 - › Document 1
 - › Machines virtuelles à importer : www.lienmini.fr/6988-301
2. Paramétrez les comptes de messagerie client ThunderBird sur les deux machines virtuelles :
 - créer les deux adresses de messagerie (M@Banque et celle du client) ;
 - créer un compte de messagerie dans ThunderBird pour chaque utilisateur ;
 - télécharger le module pour choisir le français comme langue de l'interface : Français Language Pack ;
 - ajouter le module complémentaire Enigmail dans ThunderBird afin d'intégrer le chiffrement PGP dans ThunderBird ;
 - dans le module complémentaire Enigmail, aller dans Gestion des clés et modifier les phrases de passe pour les clés de chaque utilisateur.
3. Testez l'envoi de courriels entre les deux acteurs et vérifiez si le contenu du message est crypté.
 - › Document 2
4. Téléversez les clés publiques sur un serveur de clés dédié afin d'assurer le cryptage du contenu des messages.
 - › Document 3
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.
 - › Document 4
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.

Document 1 Le schéma réseau de l'environnement de tests

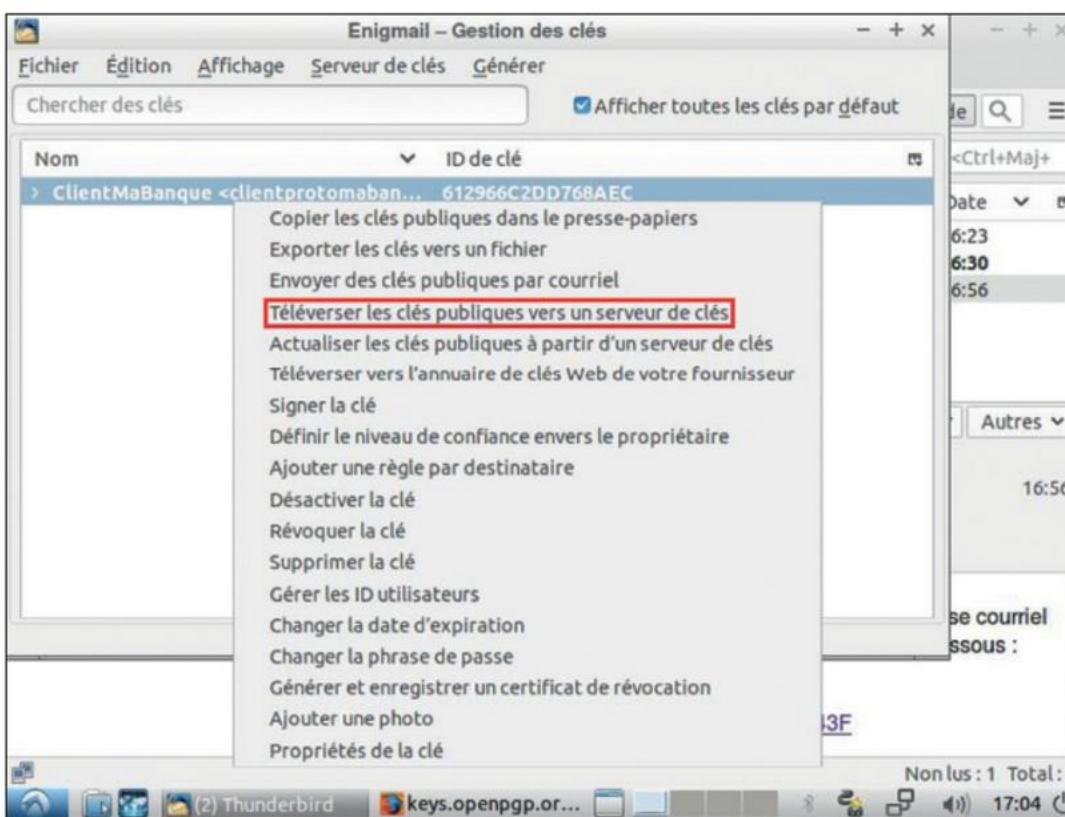


Document 2 Le cahier des charges de l'environnement de tests

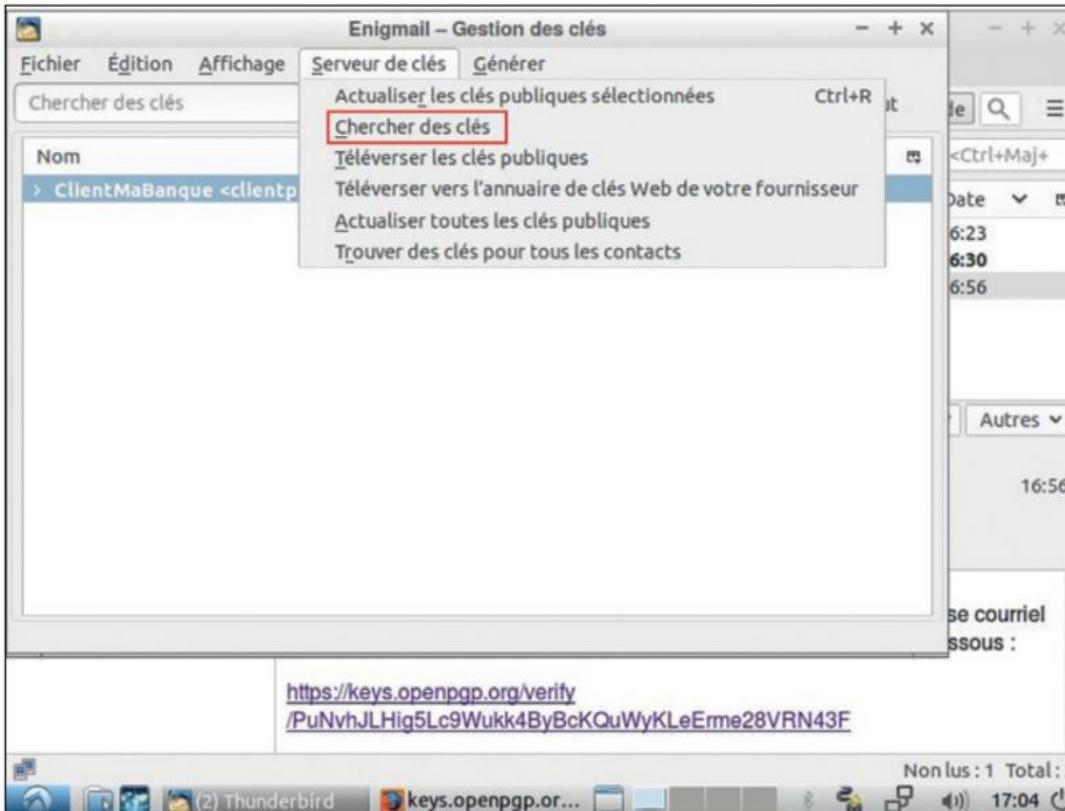
Machine virtuelle « M@Banque »	Machine virtuelle « client de M@Banque »
Système d'exploitation : Debian	Système d'exploitation : Debian
Client de messagerie : ThunderBird	Client de messagerie : ThunderBird
Nom du compte de messagerie : MaBanque	Nom du compte de messagerie : ClientMaBanque
Adresse courriel à créer : (exemple : protomabanque@gmail.com)	Adresse courriel à créer : (exemple : clientprotomabanque@gmail.com)
Phrase de passe pour le chiffrement PGP : mabanque	Phrase de passe pour le chiffrement PGP : clientmabanque

Document 3 Téléverser les clés publiques vers un serveur de clés**Première étape**

Téléverser une clé publique sur le serveur de clés

**Seconde étape**

Rechercher une clé publique sur le serveur de clés



Fiche savoirs CEJM appliquée 3

L'identité numérique de l'organisation : risques et protection juridique

I

Définitions

1. Les trois composantes de l'identité numérique d'une organisation

L'identité numérique est constituée de l'ensemble des contenus diffusés sur Internet permettant d'identifier une organisation. Trois composantes de l'identité numérique peuvent être distinguées : l'identité déclarative, l'identité agissante, l'identité calculée. Derrière chacune de ces composantes, des éléments technologiques sont sous le contrôle de la DSI, qui en assure la protection.

Composantes de l'identité numérique d'une organisation		
Identité déclarative	Identité agissante	Identité calculée
Elle regroupe les données que l'organisation choisit de partager. Elle est constituée de son nom, son logo, sa dénomination ou raison social, son adresse, sa nationalité et sa date de création. Plus largement, elle englobe toutes les informations que l'organisation décide volontairement de partager sur le Web. Exemple : un article publié sur le site de l'organisation.	Elle est constituée des métadonnées, qui permettent de mieux connaître l'organisation à travers les traces laissées par celle-ci lors de ses navigations ou de ses apparitions sur le Web. Exemple : les consultations de sites Internet pour la recherche d'un nouveau fournisseur par un membre de l'organisation.	Elle peut être définie comme l'interprétation et l'extrapolation des identités déclarative et agissante. L'analyse des données par les algorithmes permet de réaliser des projections des comportements à venir en analysant les traces laissées, volontairement ou non, par l'organisation lorsqu'elle est présente sur le Web. Exemple : le calcul du nombre de connexions sur un site pour présager de l'importance de l'activité de l'organisation.
Composantes technologiques de l'identité numérique d'une organisation		
L'IDN (<i>Internationalized Domain Name</i> , « nom de domaine internationalisé ») est le nom de domaine d'une organisation. Chaque organisation a un IDN unique sur Internet. Les certificats et les signatures électroniques sont également des éléments d'identification techniques.	Les éléments permettant de retrouver les traces laissées par l'organisation sur le Web sont l'adresse IP publique, les cookies, les données de géolocalisation ou encore les flux RSS.	Les cookies constituent généralement des sources d'informations pour les opérateurs : ils permettent d'anticiper les comportements à venir de l'organisation

2. L'e-réputation de l'organisation

L'e-réputation d'une organisation est façonnée par l'ensemble des opinions émises sur Internet en général, et sur les réseaux en particuliers. Elle repose sur les éléments d'identification numérique (traces laissées lors d'une navigation). Le service informatique doit en protéger les composantes technologiques, tel que le nom de domaine.

➤ Voir lexique BTS SIO, p. 221

...>

II

Les risques et la protection juridique de l'identité numérique

1. L'usurpation d'identité numérique

La Loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) du 14 mars 2011 définit l'usurpation d'identité comme « le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ». L'usurpation d'identité numérique concerne soit un particulier, soit une organisation. La protection contre l'usurpation d'identité passe par l'établissement d'une preuve de l'acte délictuel.

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

L'élément matériel	L'élément intentionnel
Il peut être de toute nature : nom, prénom ou toute autre donnée permettant l'identification (exemple : adresse IP). Selon l'article 226-4-1 du Code pénal, l'usurpation d'identité peut être l'action de « faire usage d'une ou plusieurs données permettant d'identifier » une personne.	L'intention de commettre un délit doit être démontrée. Il faut pouvoir prouver que l'usurpation a été réalisée « en vue de troubler la tranquillité de la victime, ou de porter atteinte à son honneur ou à sa considération ».

L'usurpation d'identité est punie d'un an d'emprisonnement et de 15 000 euros d'amende. Se servir ou tenter de se servir de l'usurpation d'identité pour commettre des actes répréhensibles est puni de cinq ans de prison et de 75 000 euros d'amende. Le texte précise que « cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne ». Il convient alors de prouver l'infraction, notamment par le biais d'un constat d'huissier qui constitue un moyen de preuve sûr pour les publications en ligne.

2. La diffamation et le dénigrement

Lorsqu'une organisation découvre que l'on porte atteinte à sa réputation, elle doit en conserver la preuve pour toute action judiciaire future. S'attaquer à l'e-réputation d'une organisation sur Internet peut s'apparenter soit à de la diffamation, soit à du dénigrement.

La diffamation	Le dénigrement
<p>La diffamation est une allégation ou une imputation d'un fait non vérifié qui porte atteinte à l'image d'une personne (physique ou morale). Elle peut être insinuée ou déguisée dans la mesure où l'on évoque une organisation identifiable sans la nommer.</p> <p>Exemple : citer la « marque à la pomme » revient à parler d'Apple, tout comme la « marque aux chevrons » pour Citroën ou le lion pour Peugeot.</p> <p>Le délai d'action est de trois mois à compter du premier jour de première publication du texte ou du contenu audio ou vidéo litigieux.</p>	<p>Le dénigrement consiste à porter atteinte aux produits ou services d'une entreprise ou à son image de marque en tenant des propos répréhensibles pouvant avoir un impact négatif sur la clientèle.</p> <p>Le dénigrement doit être poursuivi sur le fondement de l'article 1382 du Code civil dans un délai de 5 ans, à condition de rapporter la preuve d'une faute, d'un préjudice (économique) et d'un lien de causalité.</p>

Fiche savoirs CEJM appliquée 4

Le droit de la preuve électronique

Le recours à la preuve électronique est indispensable pour faire valoir ses droits dans une relation commerciale, la défense d'une propriété intellectuelle ou encore la défense de sa e-réputation.

I Définition

Extrait de l'article 1316 du Code civil :

« La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission. »

Cette définition large de la preuve permet d'adapter le droit à l'utilisation des nouvelles technologies de l'information.

II La force probante et les conditions de recevabilité de la preuve électronique

Extrait de l'article 1316 du Code civil :

« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à garantir l'intégrité. »

1. La force probante de la preuve électronique

Depuis la loi n° 2000-230 du 13 mars 2000, l'écrit électronique est accepté comme preuve légale au même titre que l'écrit papier, ce qui lui confère sa force probante.

La force probante est la valeur juridique donnée à un mode de preuve même si le juge reste libre de forger son intime conviction, avec l'obligation de motiver sa décision.

2. Les conditions de recevabilité de la preuve électronique

Deux conditions doivent être respectées pour qu'une preuve électronique soit recevable :

- l'authentification de la personne à l'origine de la preuve doit être rendue possible ;
- l'intégrité de la preuve doit être garantie.

III Les moyens de la preuve électronique

1. Les moyens/supports de l'authentification

L'article 1316-4 du Code civil stipule que la « signature identifie celui qui l'appose et manifeste le consentement des parties aux obligations qui découlent de l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».

La signature électronique est recevable à condition que le signataire soit identifié et que l'écrit soit indissociable de celle-ci. Elle permet de garantir la non-répudiation par le signataire du document signé, c'est-à-dire le fait que le signataire ne peut contester être l'auteur de l'écrit.



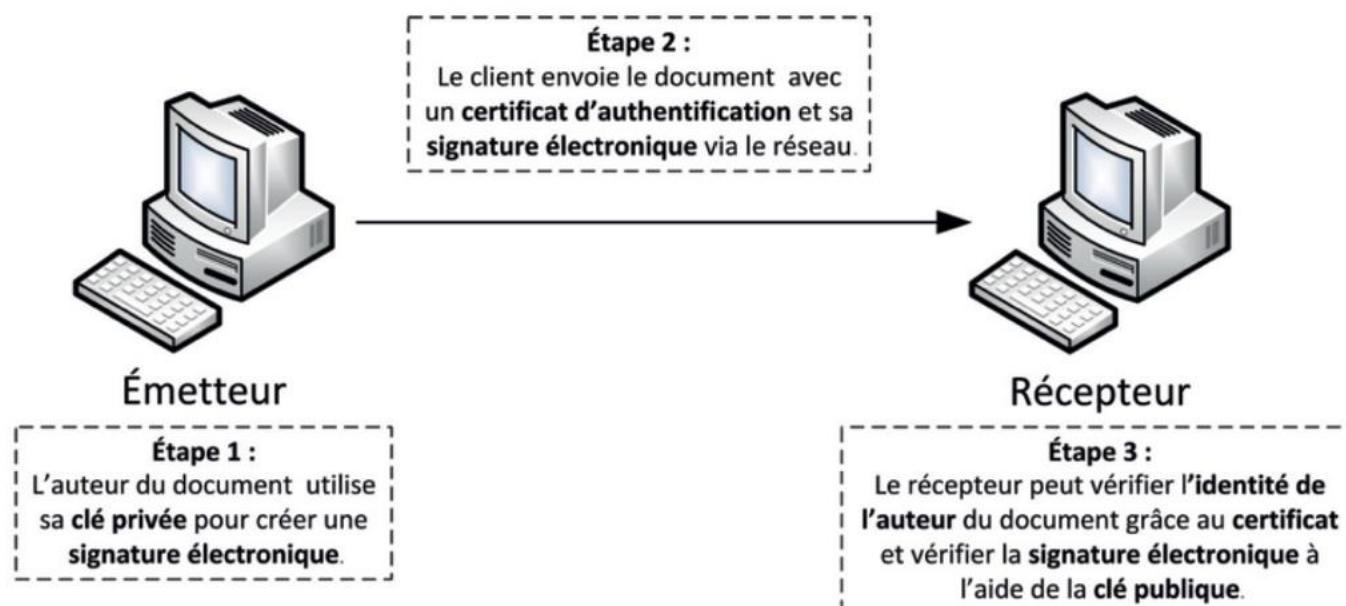
Une signature électronique est réalisée à partir de la cryptographie asymétrique (voir Fiche savoirs technologiques 9, p. 151). Elle repose sur un couple de clés, l'une privée, connue par son seul propriétaire, l'autre publique, connue de tous. La clé publique a pour fonction de crypter le message, et la clé privée de le déchiffrer.

La problématique est de pouvoir vérifier l'identité de l'auteur de la signature. L'utilisation d'un certificat électronique, délivré par une autorité de certification de confiance, permet de répondre à ce besoin.

Un certificat doit contenir :

- les informations d'identification (par exemple, le nom, la localisation) ;
- une clé publique ;
- une signature construite à partir de la clé publique.

Échange d'un document avec signature électronique et certificat d'authentification



2. La garantie de l'intégrité de la preuve électronique

L'intégrité attendue d'une preuve électronique est assurée par l'utilisation d'un algorithme de chiffrement qui permet de vérifier, à l'arrivée du message signé électroniquement, que celui-ci n'a pas été modifié.

Le procédé technique de calcul d'empreintes électroniques (par exemple, MD5 ou SHA) de l'information source et de l'information copiée est un moyen incontestable de respecter ce critère : il permet de démontrer que ces informations n'ont pas pu être altérées au moment de cette opération et que le contenu est resté strictement identique.

3. Les documents électroniques recevables comme preuves électroniques

Les documents signés certifiés par un organisme d'État	Les documents non signés	Les courriels, les SMS et les MMS
Ces documents signés garantissent l'identification de l'auteur (signature électronique) et l'intégrité du document par l'utilisation d'un certificat électronique délivré par l'État. Ils constituent des documents électroniques authentiques.	L'auteur du document est identifiable mais sans signature apparente. Cependant, l'intégrité est assurée par un procédé fiable. Exemple : l'échange de données informatisées.	Les documents électroniques tels que les courriels, les SMS et les MMS ne permettent pas l'identification de l'auteur et ne garantissent pas l'intégrité du message. Ils ne peuvent pas être assimilés à des écrits, et encore moins à des écrits « parfaits ».

Les risques des cyberattaques pour l'organisation

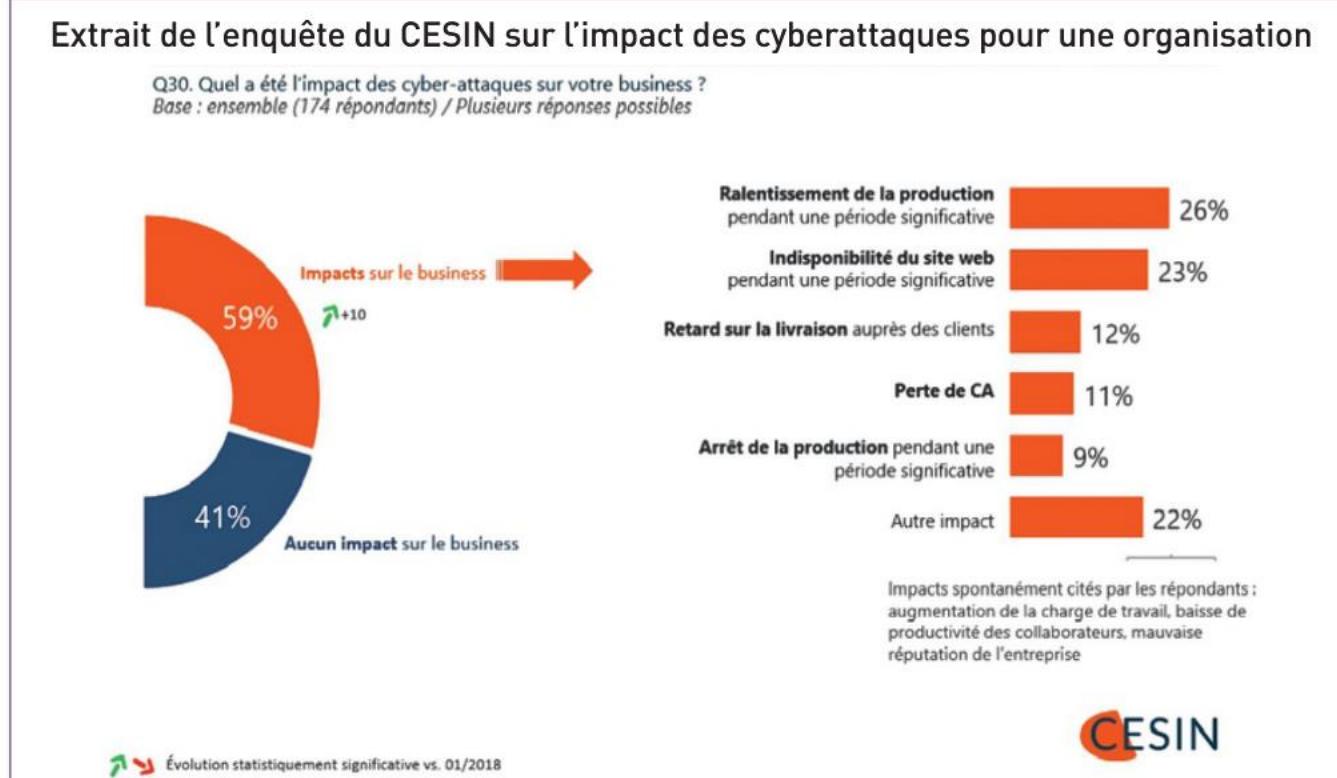
D'après une étude du CESIN (Club des experts de la sécurité de l'information et du numérique), 80 % des entreprises interrogées déclare avoir fait l'objet d'une cyberattaque. Les objectifs des cyberattaques sont multiples : demandes de rançons, fraudes externes, défigurations de sites Web, vols ou fuites d'informations, cyberespionnage économique ou industriel. Les entreprises victimes de ces types d'attaques risquent des conséquences économiques ou juridiques, ou encore une atteinte de leur identité.

I

Les risques économiques des cyberattaques

1. Un impact fréquent

Une enquête démontre que 60 % des cyberattaques ont des conséquences directes sur l'activité économique de l'entreprise. Le ralentissement de la production et l'indisponibilité du site Web de l'organisation sont les deux risques majeurs, représentant respectivement 26 % et 23 % de l'ensemble des impacts.



2. Le calcul économique du risque acceptable

La prise en compte des risques découle des résultats d'une analyse méthodologique (par exemple, la méthode **E BIOS**, voir fiche méthode 5, p. 211) et d'un calcul de coûts par le chef d'entreprise.

On mesure le risque acceptable en comparant le coût des solutions à mettre en œuvre pour sécuriser le système d'information et les coûts qu'un sinistre pourrait entraîner. Le choix d'investissement pour les solutions envisageables peut être le transfert d'une partie des risques vers un assureur spécialisé.

➤ Voir lexique BTS SIO, p. 221

…>

II

Les risques juridiques des cyberattaques

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, elle doit pouvoir apporter des preuves.

Les utilisateurs disposent de deux types de recours contre une organisation qui ne respecte pas ses obligations légales :

- un recours civil : demande de dommages et intérêts pour réparer le préjudice. L'utilisateur doit alors prouver le préjudice ;
- un recours pénal : demande de sanctions en cas vol de données et défaut du respect des précautions utiles pour préserver la sécurité des données.

Par ailleurs, les cyberattaques sont par nature susceptibles de causer des dommages en cascade du fait de l'interdépendance des réseaux informatiques entre partenaires commerciaux (fournisseurs, clients, etc.). Ces partenaires peuvent se prévaloir de possibles manquements aux nouvelles obligations mises à la charge du responsable de traitement et du sous-traitant pour rechercher la responsabilité contractuelle de l'entreprise.

III

Les risques d'atteinte à l'identité de l'entreprise

1. L'usurpation d'identité

L'usurpation d'identité est l'un des risques majeurs pour les organisations.

Le cas d'escroquerie le plus développé et qui ne nécessite pas de compétences techniques est celui de la fraude au président. Cette opération consiste à se faire passer pour le dirigeant d'une entreprise afin d'obtenir une somme d'argent de la part d'un des employés de l'entreprise par le biais d'un virement bancaire, vers un compte souvent situé à l'étranger. Le hameçonnage (phishing, en anglais) est un autre cas d'escroquerie. L'escroc adresse des milliers de courriels à des internautes afin de collecter des données sensibles ou personnelles en usurpant l'identité numérique d'une organisation.

De telles pratiques sont des infractions pénales : délits d'usurpations d'identités (article 226-4-1 du Code civil) et escroqueries (article 313-1 du Code civil). En se portant partie civile, l'entreprise pourra obtenir réparation de son préjudice.

2. La défiguration d'un site Internet

La défiguration est l'altération par un pirate de l'apparence d'un site Internet. Durant l'attaque, le site n'est souvent plus utilisable, ce qui peut entraîner des pertes directes de revenus et de productivité. Par ailleurs, en étant visible publiquement, la défiguration démontre que l'attaquant a pu prendre le contrôle du serveur et, donc, accéder potentiellement à des données sensibles. Cela porte directement atteinte à l'image et à la crédibilité du propriétaire du site auprès de ses partenaires.

IV

Le risque humain et écologique

Les attaques sur des systèmes de contrôle des installations d'organisations produisant ou manipulant des produits dangereux peuvent constituer des risques pour l'intégrité physique des hommes ou pour l'environnement naturel.

➤ Voir lexique BTS SIO, p. 221

1 QCM



Retrouvez ce QCM
en version interactive
www.lienmini.fr/6988-302

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



› Fiche CEJMA 3

- 1 Retrouvez la composante de l'identité numérique visée par la cyberattaque de Tradec.
- 2 Décrivez brièvement chaque étape de la cyberattaque contre Tradec (annexe).



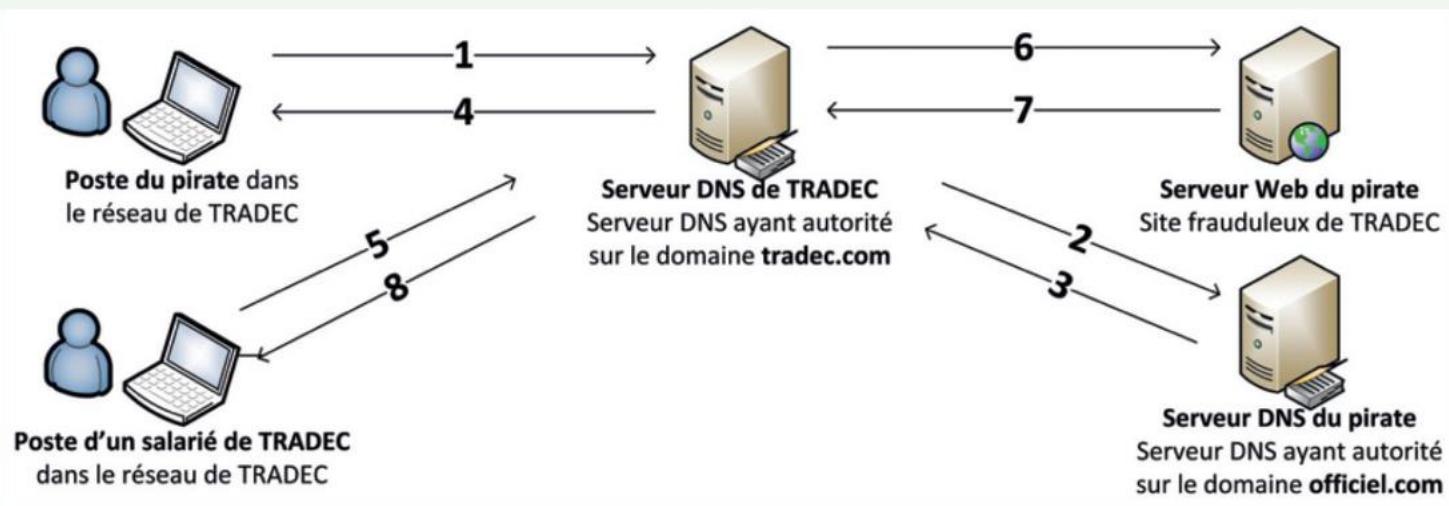
Annexe

L'historique de la cyberattaque réalisée par la DSI de Tradec

C'est dans le cadre de son travail quotidien que le laboratoire Tradec a détecté, vendredi 10 juin, vers 18 h, une attaque de type «empoisonnement du serveur DNS» (*DNS Poisoning*).

Les experts du laboratoire ont découvert, avec surprise, que ce n'était pas le site Web commercial de Tradec qui était touché, mais son serveur DNS. En effet, le serveur dirigeait à tort des requêtes à destination du site Internet de Tradec vers un site Internet marocain hébergé en Belgique.

Dans le cas de l'attaque détectée, c'est le serveur DNS qui disposait de correspondances adresse IP / nom de domaine volontairement erronées. En conséquence, l'ensemble des requêtes qui étaient effectuées auprès de ce serveur DNS répercutait une fausse information en indiquant que le nom de domaine de Tradec correspondait à une adresse IP localisée en Belgique. Heureusement, la cyberattaque a été détectée rapidement par la DSI. Cela a permis d'éviter que le pirate ne crée une copie à l'identique du site visé en vue de récupérer, par exemple, des noms d'utilisateurs et mots de passe.



3**Simuler un empoisonnement du serveur DNS**

➤ Fiche CEJMA 3

Situation

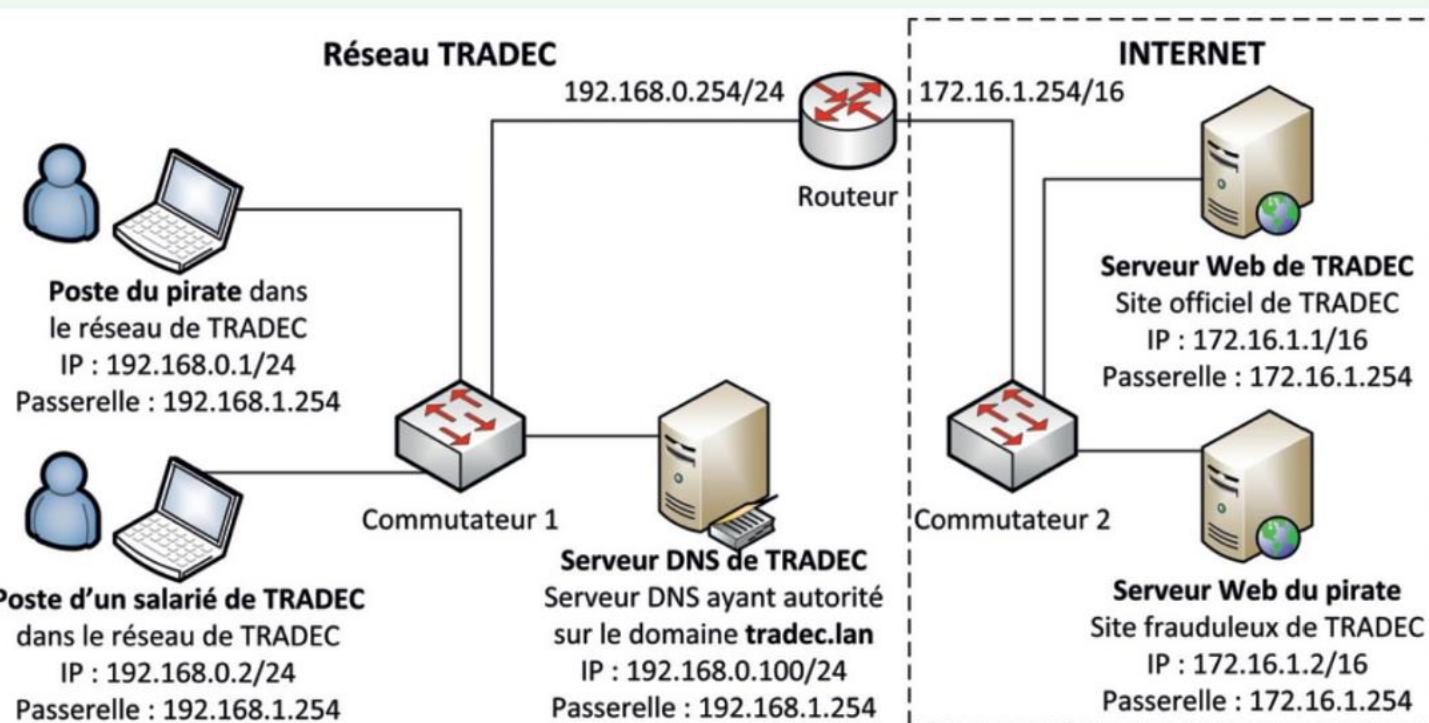
Afin de sensibiliser vos collègues de la DSI de Tradec au problème de l'empoisonnement du serveur DNS, vous décidez de leur montrer comment fonctionne ce type d'attaque en proposant une simulation dans un environnement de test.

Pour simplifier la démonstration, vous allez créer un script dans un langage que vous choisissez et dont l'objectif est de modifier la résolution de la zone DNS dans le serveur DNS.

Ainsi, la résolution doit être :

- avant l'utilisation du script : 172.16.1.1/16 pour le nom du site tradec.lan ;
- après l'utilisation du script : 172.16.1.2/16 pour le nom du site tradec.lan.

- 1** Réalisez la maquette de votre environnement de test à l'aide du simulateur Packet Tracer.
- 2** Mettez en place l'environnement de tests en respectant le cahier des charges (annexe 2).
- 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 de Tradec.
- 4** Réalisez les tests d'accès au site tradec.lan depuis le poste du salarié.
- 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.

Annexe 1 Le schéma du prototype à mettre en place**Annexe 2** Le cahier des charges

L'environnement de tests doit respecter les conditions suivantes :

- chaque poste doit disposer de ses configurations réseau (IP, IP de la passerelle, IP du serveur DNS) ;
- le service DNS (sous Linux ou Windows) doit être installé sur le serveur DNS de Tradec ;

- deux commutateurs doivent permettre de relier les postes (un seul peut suffire avec la création de deux VLANs différents et un routage inter-VLANs) ;
- le routeur doit permettre le trafic entre le réseau Tradec et le réseau Internet.

➤ Voir lexique BTS SIO, p. 221

4

Déployer la signature électronique comme moyen de preuve



› Fiches CEJMA 4 et 5

Situation

Initiée par les banques en ligne, puis généralisée à l'ensemble du secteur bancaire, la signature dématérialisée est l'une des principales innovations intervenues dans le cadre de la numérisation des services bancaires. Le client peut désormais signer son contrat depuis chez lui, par SMS ou messagerie vocale, économisant ainsi temps et argent, avec un meilleur suivi. De plus, contrairement à certaines idées reçues, la signature dématérialisée est complètement sécurisée.

- 1** Indiquez sous quelles conditions la signature électronique proposée par Fortuneo est une preuve aussi recevable qu'un écrit papier.
- 2** Expliquez le rôle de la signature électronique et indiquez comment on peut la vérifier.
- 3** Analysez les avantages de l'utilisation de la signature électronique pour Fortuneo et pour ses clients.
- 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.

Annexe

La signature électronique : comment ça marche ?

La signature électronique est gérée par votre banque, qui vous remet un certificat numérique prenant généralement la forme d'un «logiciel de signature» envoyé sur votre ordinateur ou votre téléphone. Ce dernier contient une série de données telles que votre identité, celle de l'établissement bancaire émetteur, une clé privée et une clé publique, qui servent à crypter et décrypter la signature.

Ce logiciel crée ensuite une empreinte numérique composée d'une suite de lettres et de chiffres qui est codée grâce à la clé privée contenue dans le

certificat numérique. Toutes les données fusionnent alors pour créer la signature numérique.

Et concrètement, chez Fortuneo, il vous suffit par exemple d'initier une souscription pour recevoir un SMS sur le numéro renseigné. Vous devez ensuite :

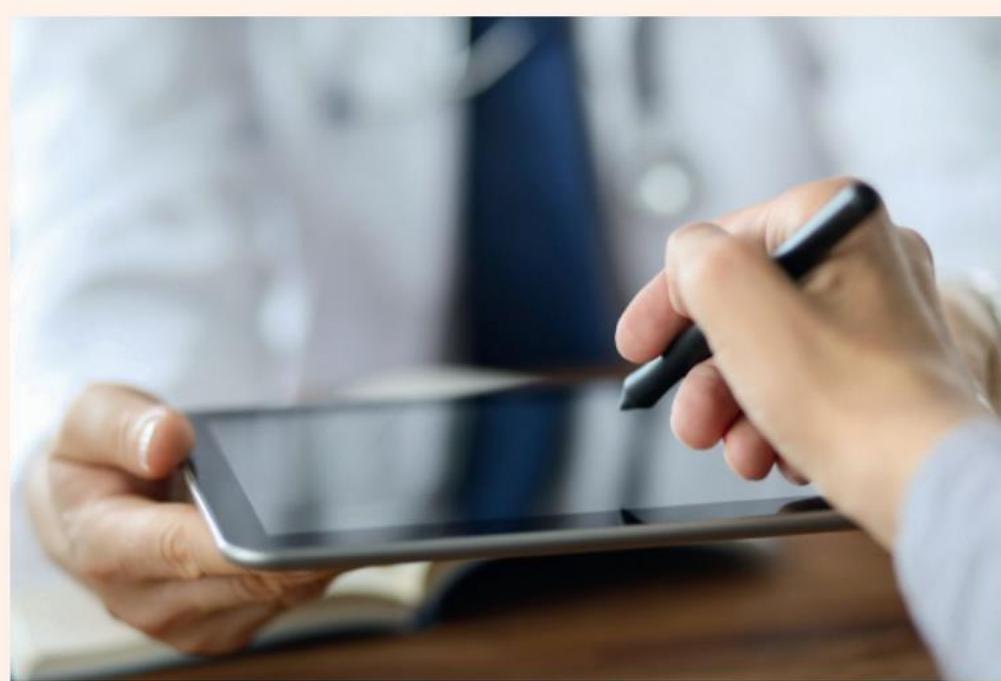
- entrer le code reçu dans la zone correspondante ;
- puis, valider la signature du contrat.

Sur le plan juridique, la signature dématérialisée 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.

www.fortuneo.fr



Évaluation 2

L'organisation cliente

La marque de prêt-à-porter haut de gamme Léandre & Lysandre, née en 2009, compte dix établissements dans les grandes villes de France. Elle a ouvert, en janvier dernier, sa onzième boutique à Strasbourg. Tout d'abord destiné aux enfants, Léandre & Lysandre a ensuite élargi son offre aux adolescents.

Sa stratégie commerciale est basée sur une démarche marketing multicanale associant des canaux de distribution (magasins et sites Web) et des canaux relationnels, notamment réseaux sociaux. Depuis quelques semaines, des publications sur Facebook proposent des bons de réduction pour des vêtements de la marque. Or, l'entreprise n'est pas à l'origine de cette campagne.

Le prestataire informatique

M^{me} Chevance est RSSI (responsable de la sécurité du système d'information). Elle assure la protection de l'identité numérique de Léandre & Lysandre.



Votre mission

Recruté(e) pour assister M^{me} Chevance, vous devez vérifier si l'entreprise fait face à une attaque de type hameçonnage et déployer des moyens de preuve électronique de cet acte de malveillance. Pour réaliser ce travail, vous vous appuyez sur le dossier documentaire mis à votre disposition.

Missions

1

Protéger l'identité numérique de l'organisation suite à une attaque par usurpation d'identité

M^{me} Chevance s'interroge sur la responsabilité de la société dans cette fausse campagne publicitaire. Elle vous demande de rassembler les éléments démontrant une attaque de type hameçonnage et d'en mesurer les risques sur l'identité numérique de l'organisation. .

- 1.1. Repérez les éléments dans le coupon de réduction qui permettent de reconnaître une opération d'hameçonnage.
- 1.2. Identifiez la stratégie utilisée pour obtenir les données personnelles des clients.
- 1.3. Identifiez les conséquences pour Léandre & Lysandre de tous ces avis négatifs publiés sur les réseaux sociaux suite à cette cyberattaque.

2

Déployer les moyens appropriés de preuve électronique

Le coupon de réduction imitant la charte graphique et le lien vers le site Internet semblent pour M^{me} Chevance être des éléments suffisants pour justifier un dépôt de plainte. Elle vous demande de l'aider à monter le dossier et de la conseiller face à cette situation.

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

Dossier documentaire

Document 1

Le faux coupon de réduction diffusé sur Facebook



Document 2

Message en suivant le lien vers le questionnaire

Félicitations !

Vous avez été qualifié pour obtenir votre coupon de 50€
Pour recevoir ce coupon, suivez les dernières étapes ci-dessous :

1. Partagez cette page en cliquant sur le bouton « PARTAGER » et écrivez « Merci » dans le champ des commentaires.
2. Cliquez sur « Recevoir le coupon », entrez vos coordonnées et répondez à 2 questions sur la marque.

Partager avec vos amis sur Facebook

Recevoir le coupon

Document 3

L'ingénierie sociale pour le piratage psychologique

Le hacker Kevin Mitnick a théorisé et popularisé la pratique de manipulation psychologique qui repose sur les failles humaines d'un système d'information pour briser ses barrières de sécurité. Le piratage

psychologique vise à soutirer frauduleusement des informations à l'insu de son interlocuteur. L'appât du gain peut ainsi être un moyen de mettre en confiance une cible et de lui soutirer des informations personnelles.

Document 4

Mentions légales et obligatoires pour garantir la validité d'un coupon

1. Montant de la réduction en euros
2. Date de fin de validité
3. Nom et RCS de l'émetteur
4. Visuel et nom du produit
5. Modalités d'application de la réduction : produit, conditions claires et lisibles, limitation géographique, limitation d'enseigne le cas échéant
6. Code coupon et mention « Traitement ScanCoupon » encadrée de deux ronds noirs, indispensables pour identifier le centre de traitement habilité à traiter le bon et faciliter le scanning en caisse.

Document 5

Avis posté par un client sur les faux coupons



BeauGosse68

@BG68



Suivre

@2L Coupon 50€ refusé en magasin C'est quoi cette arnaque ?

#FauxCoupon

12 :23 – 10 février 2020

247

884

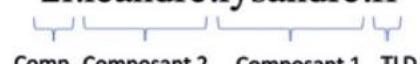
492

Document 6

La structure du nom de domaine de Léandre & Lysandre

Un nom de domaine est composé de plusieurs parties, séparées par des points. Ces différents composants se lisent de droite à gauche.

21.leandre.lysandre.fr



- TLD (*Top-Level Domain* ou domaine de premier niveau). Le TLD fournit une information générique purement indicative sur le service associé au nom de domaine. Certains TLD peuvent indiquer que le site ou service provient d'un pays donné (par exemple : .us, .fr ou .sh qui correspondent aux États-Unis, à la France et à Sainte-Hélène). D'autres TLD sont génériques (par exemple : .com, .org, .net).

- Composant : les composants sont les différents fragments d'un nom de domaine (le TLD est le premier composant). Un composant peut être une lettre ou une phrase entière (sans espace). Ce composant situé juste après le TLD est parfois appelé « domaine de deuxième niveau » (ou *Secondary Level Domain* – SLD – en anglais). Un nom de domaine peut avoir plusieurs composants.

Document 7

Les violations de données personnelles

- L'article 226-18 du Code pénal dispose que : « Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. ».
- Les entreprises dont l'identité a été usurpée sont considérées comme des victimes et peuvent également agir, selon les cas, sur le terrain de la contrefaçon, celui de la diffamation ou encore de l'injure.
- La loi Loppsi II de 2011 a créé un délit d'usurpation d'identité (art. 226-4-1 du Code pénal) : « Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne ».
- Les consommateurs ont la possibilité de s'appuyer sur les articles du Code monétaire et financier pour limiter leur préjudice financier en cas d'utilisation de leurs données bancaires à des fins d'opérations de paiement non autorisées.

Document 8

Le coût d'une cyberattaque

Une entreprise spécialisée dans la vente en ligne s'est fait voler plus de 2 millions de données clients sensibles en 2009. Elle a dû fermer momentanément son site Web (coût : 1,5 million d'euros), répondre aux demandes d'indemnisation des banques des clients touchés (1 million d'euros), assumer des expertises, des notifications et des exercices de veille (1,25 million d'euros), et enfin travailler à restaurer sa notoriété (250 000 euros). Une facture totale de plus de 4 millions d'euros.

Document 9

Usurpation d'identité sur internet : comment réagir ?

Si vous souhaitez que la personne qui a usurpé votre identité soit identifiée et poursuivie, il faut déposer une plainte auprès des services de police, de gendarmerie ou du procureur de la République car il s'agit d'une infraction pénale. Si des informations ou des propos ont été publiés sur Internet en votre nom par l'usurpateur, demandez leur suppression directement au responsable du site.

Dans tous les cas,

- si l'usurpation vous semble avérée, constituez un dossier avec les éléments déterminant qu'il s'agit bien de vos propres informations et non de celles d'un homonyme ;
- relevez les adresses URL des pages/profils concerné(e)s ;
- conservez des captures d'écran du faux profil et de ses publications ;
- préparez les justificatifs qui vous semblent pertinents.

www.cnil.fr

Contexte 3

Sécuriser les équipements et les usages des utilisateurs



L'organisation cliente

La commune de Marut, dans le Cantal, qui compte 1 900 habitants, a créé en janvier 2012 une Maison de services au public (MSAP). Cette structure permet aux habitants d'accéder à un service de proximité et/ou de bénéficier d'un accompagnement administratif dans de nombreux domaines de la vie quotidienne, avec l'aide d'agents médiateurs. Enedis, la Mutuelle agricole, les caisses d'assurance maladie, de retraite ou d'allocations familiale, les

Impôts, le Centre local d'information et de coordination (CLIC) sont ainsi accessibles depuis la MSAP.

Les ressources numériques sont utilisées par un public très varié, ce qui peut occasionner des problèmes de sécurité du système d'information. M. Brillat, directeur de la structure, veut donc réaliser un audit de sécurité afin d'identifier les failles du système et apporter des solutions pour y remédier.

Le prestataire informatique

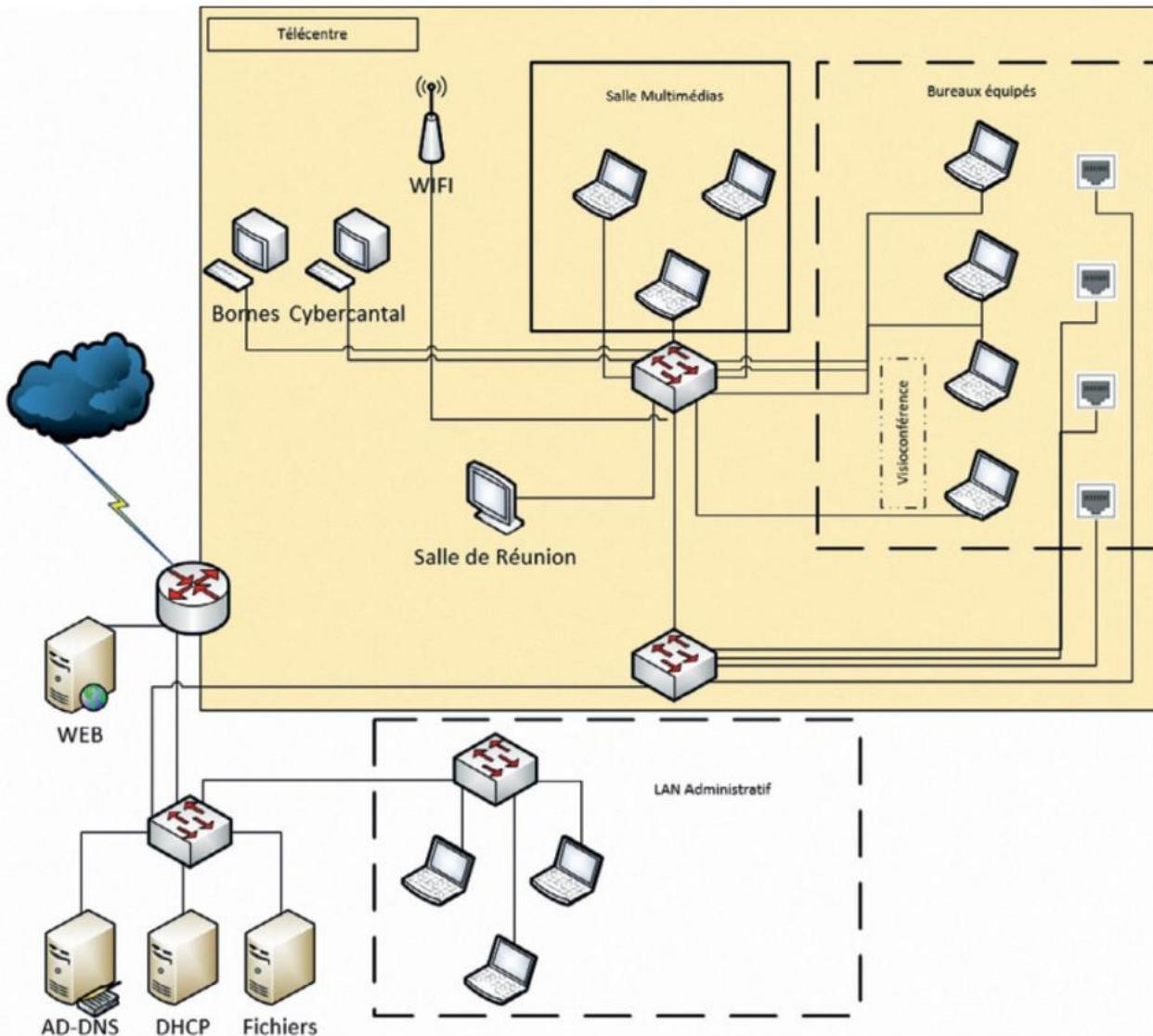
HDesk'63 est un centre de services en technologies de l'information, fondé en janvier 1999 et implanté dans la zone commerciale d'Aubière, à Clermont-Ferrand, dans le Puy-de-Dôme. Son objectif est d'assurer un fonctionnement optimal des infrastructures de réseaux de ses clients et d'apporter un support aux utilisateurs via son centre

d'appel. HDesk'63 peut, à la demande d'une organisation, fournir une délégation de personnel pour aider à renforcer ses équipes dans le cadre de projets spécifiques. La direction des systèmes d'information (DSI) de HDesk'63 est dirigée par M. Hiram.

Contexte 3

Description du SI de l'organisation

Schéma général du réseau de la MSAP



Cahier des charges

Afin de garantir un accès sécurisé aux ressources et une protection des données des utilisateurs, un audit de sécurité est effectué à la demande de la MSAP de Marut pour contrôler :

- la robustesse des éléments d'authentification des utilisateurs ;

- la sécurité des postes de travail ;
- la sécurité des serveurs ;
- la surveillance des mises à jour et des correctifs des applications ;
- les connexions réseaux ;
- les droits d'accès et priviléges des utilisateurs.

Votre mission

Vous êtes accueilli(e) au sein de HDesk'63 en tant que technicien(ne) support aux utilisateurs afin de répondre à la demande de l'organisation cliente représentée par la commune de Marut. Vous vous rendez dans les locaux de la MSAP afin de réaliser un audit de sécurité du système d'information. M. Brillat pense également qu'il serait utile de sensibiliser l'ensemble des utilisateurs aux bons usages des outils numériques.

Informer les utilisateurs et mettre en œuvre les défenses appropriées

COMPÉTENCES

- Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter
- Identifier les menaces et mettre en œuvre les défenses appropriées

SAVOIRS ASSOCIÉS

- Sécurité des terminaux utilisateurs et de leurs données : principes et outils
- La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique

Situation professionnelle

M. Brillat, le directeur de la MSAP, sollicite HDesk'63 pour identifier les failles de sécurité potentielles liées aux pratiques des utilisateurs du télécentre. Il souhaite également des recommandations sur les solutions techniques de défense des équipements.

M. Hiram, votre directeur, vous confie les différentes missions de ce projet. Vous êtes chargé(e) d'informer les utilisateurs de la MSAP sur les **risques** associés à l'utilisation des ressources numériques du télécentre. Vous devez également identifier les menaces inhérentes à l'utilisation du télécentre en vue d'apporter les défenses appropriées.



➤ Voir présentation générale, p. 83

Missions professionnelles

1

Informer les utilisateurs sur les risques et promouvoir les bons usages à adopter



M. Brillat souhaite compléter la charte informatique en vigueur dans la MSAP. Il est en effet nécessaire d'y insérer une rubrique sur les bonnes pratiques numériques, afin d'informer les utilisateurs du SI sur les risques associés à son utilisation et promouvoir les bons usages à adopter. Votre première mission consiste à réaliser un diagnostic des menaces inhérentes à l'utilisation du SI de la MSAP, liées à l'authentification et aux pratiques courantes telles que la lecture des courriels et l'utilisation d'applications métiers. Dans un second temps, vous complétez la charte informatique de la MSAP en y intégrant une rubrique «Bonnes pratiques numériques».

Travail à faire

Vous disposez du relevé d'informations réalisé d'après l'observation des activités journalières des utilisateurs du télécentre (documents 1 à 4).

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

- > [Fiche savoirs technologiques 4](#)
- > [Documents 1, 2, 3 et 4](#)

Vos observations ont permis de mettre en évidence un certain nombre de failles de sécurité dans le SI. Vous proposez des solutions pour y remédier.

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

- > [Fiche savoirs technologiques 4](#)
- > [Documents 5 et 6](#)

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

- > [Fiche savoirs technologiques 4](#)
- > [Document 7](#)

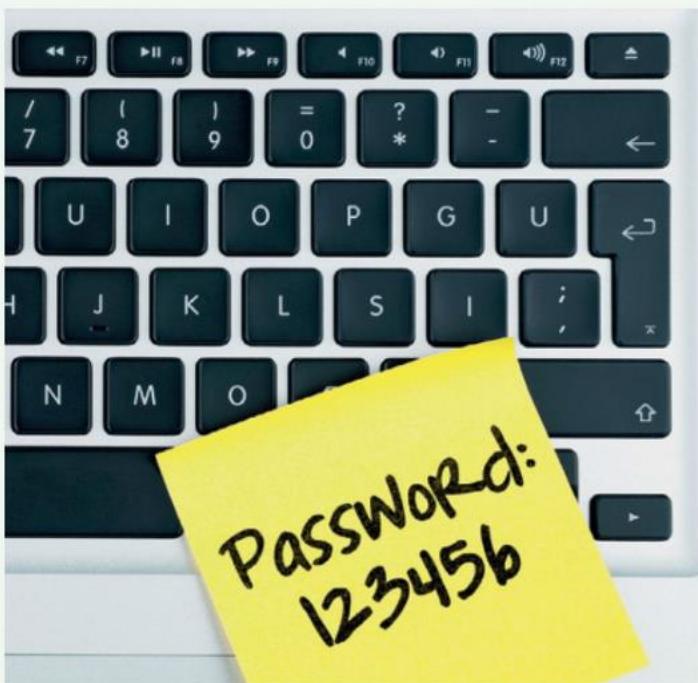
Un des axes de votre mission consiste à compléter la charte informatique de la MSAP en rédigeant la rubrique consacrée aux bonnes pratiques à adopter dans l'utilisation des outils numériques.

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

- > [Fiche savoirs CEJMA 6](#)
- > [Document 8](#)

Dossier documentaire

Document 1 Le mot de passe utilisé par le prestataire Enedis



Document 2 La stratégie d'authentification pour accéder au SI de la MSAP

Les utilisateurs du SI de la MSAP qui désirent accéder aux services proposés par le télécentre doivent, dans un premier temps, réserver la ressource numérique souhaitée auprès de M. Jivon, l'administrateur réseau. Ce dernier intervient alors sur l'**Active Directory** (service centralisé d'identification et d'authentification pour un réseau d'ordinateurs utilisant le système Windows) pour créer un compte qui a pour identifiant le nom de l'organisme. À la première connexion, l'utilisateur est invité à modifier son mot de passe. Ainsi, pour toutes les prochaines réservations, l'intervenant possédera ses données de connexion.

Document 3 Nomadisme et service BYOD dans le télécentre

BYOD (de l'anglais *Bring Your Own Device*) est une pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette électronique) dans un contexte professionnel. Les utilisateurs de la MSAP y sont autorisés dans le cadre de leurs missions. Dans ce cas, les partenaires (CLIC, MSA, etc.) sont en charge de la configuration de leurs applications.

M. Jivon n'a aucun moyen de vérifier la configuration de ces unités nomades. Si les partenaires de la MSAP souhaitent imprimer des documents, ils doivent les enregistrer sur un support amovible et se rendre au service reprographie pour l'impression. Un mot de passe leur est alors communiqué pour avoir accès à l'imprimante.



Missions professionnelles

Document 4 Un courriel reçu par la MSAP

La personne qui assure la permanence de la MSAP a cliqué sur le lien entouré ci-dessous.

De : Free@gmail.com
 À : permanence-marut@msap.fr
 Envoyé : Jeudi 11 décembre 2020 01.04.02
 Objet : Notification SZ27503S



Réf. : F4753898/26321908#0
Votre identifiant abonné : 4753898

Paris, le 11/12/2011

Madame, Monsieur,

Il a été porté à notre attention que vos informations de facturation Freebox ne sont plus à jour.
 Pour cela nous vous prions d'accéder à votre espace personnel par le lien ci-dessous, et de mettre à jour toutes vos informations personnelles afin que vous aidiez à certifier votre compte.

Accédez à votre compte ici

Document 5 Un exemple de bonne pratique dans l'utilisation d'un mot de passe

Sur le site *How Secure Is My Password* (<https://howsecureismypassword.net>), la résistance du mot de passe **msap15** a été testé.

Le résultat de ce test indique :

QUELLE EST LA SÉCURITÉ DE MON MOT DE PASSE?

.....

Cela prendrait à un ordinateur
54 MILISECONDES
pour trouver votre mot de passe

Un second test a été réalisé en ajoutant à ce mot de passe le caractère spécial « , » et en remplaçant le « a » par le signe « @ » : **Ms@p,1500**.

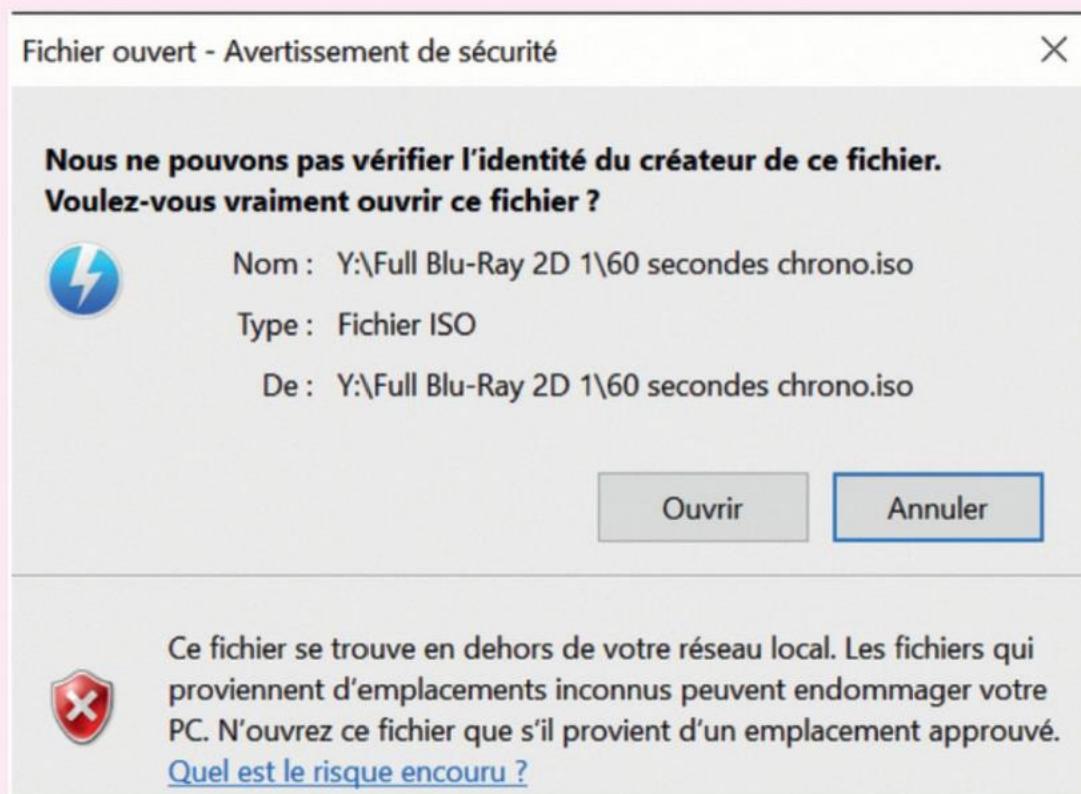
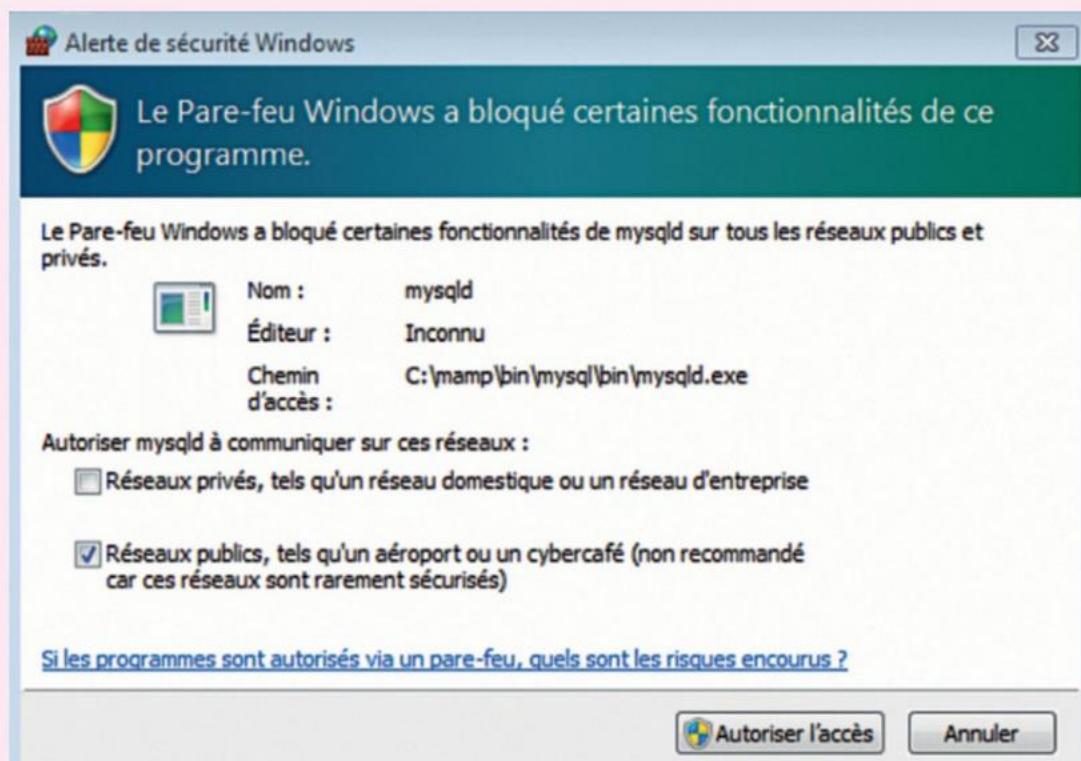
QUELLE EST LA SÉCURITÉ DE MON MOT DE PASSE?

.....

Cela prendrait à un ordinateur
7 MOIS
pour trouver votre mot de passe

Document 6 Deux alertes de sécurité

Choisir la bonne réponse en cliquant sur le bouton approprié.



Document 7 Relevé d'utilisation d'une messagerie

M^{me} Asarchoun, chargée de clientèle à la MSAP, traite tous les jours les demandes d'informations de ses clients par courriel. Voici comment elle utilise sa messagerie professionnelle.



Missions professionnelles

Document 8 Un extrait de la charte informatique de la MSAP

MSAP de la commune de Marut

Charte informatique

Introduction

Cette charte a pour vocation de présenter les bonnes pratiques à adopter au sein du système d'information de la MSAP et, plus particulièrement, au niveau du télécentre. Elle stipule les droits et devoirs de chaque utilisateur.

1. Ressources mises à disposition

Chaque utilisateur peut avoir accès à un espace de travail privatif ou collectif, avec une connexion Internet, un environnement bureautique Windows, un espace de reprographie et enfin une salle de visioconférence et de réunion. Un espace de stockage privatif est proposé sur le serveur de fichiers de la MSAP.

2. Les règles de sécurité en vigueur

a. Authentification sur les postes de travail

Chaque utilisateur se voit attribuer un identifiant qui lui permettra de définir son mot de passe. L'identifiant est nominatif et ne peut être partagé avec un autre utilisateur. Le mot de passe est strictement confidentiel, le propriétaire est responsable de l'utilisation qui en est faite et s'engage à ne pas le communiquer à un tiers.

b. Configuration des environnements de travail

La configuration des postes de travail fournie dans les différents espaces de travail permet d'assurer la sécurité des utilisateurs et de leurs données. Il ne faut pas intervenir sur l'installation automatique des **correctifs**.

c. Environnement Internet

La connexion à certains sites pourrait fragiliser la sécurité du SI de la MSAP. Il faut donc être particulièrement vigilant dans la gestion de sa boîte de courriels professionnelle.

3. Conditions particulières liées à l'utilisation des outils nomades

L'utilisation des supports numériques personnels est autorisée. Cependant, leur configuration doit garantir la sécurité du SI de la MSAP. Ces supports ne doivent être utilisés que dans le cadre professionnel. Les téléchargements illicites sont interdits.

Je soussigné, , utilisateur des ressources numériques proposées par la MSAP de la commune de Marut, certifie avoir pris connaissance de la charte des bons usages de l'utilisation du SI de la MSAP, des droits et obligations qui en découlent et atteste que je suivrais les instructions précisées dans celle-ci.

Date :

Signature

➤ Voir lexique BTS SIO, p. 221

Missions professionnelles

2

Identifier les menaces et mettre en œuvre les défenses appropriées

Vous avez identifié un certain nombre de mauvaises pratiques qui provoquent des failles de sécurité et favorisent des attaques du SI. À la demande de M. Brillat, vous devez à présent apporter des solutions techniques pour protéger la MSAP.

Votre mission consiste à réaliser un diagnostic des moyens de défense déjà en place et à vérifier si les configurations sont adéquates. Vous disposez d'un relevé d'informations des configurations des postes de travail des bureaux de la MSAP, ainsi que de ceux relevant des pratiques BYOD.



Travail à faire

Dans un premier temps, vous réalisez un diagnostic des configurations actuelles.

1. Précisez la fonction de chacune de ces configurations.

- > Fiche savoirs technologiques 4
- > Documents 1, 2 et 3

Vos observations ont permis de mettre en évidence des failles de sécurité.

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

Le document 4 présente les différents outils installés sur quelques postes de travail de la MSAP. Vous préconisez à M. Brillat le déploiement de l'ensemble de ces outils sur tous les postes afin d'obtenir un parc homogène et plus sécurisé.

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

- > Fiche savoirs technologiques 4
- > Document 4

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

- > Fiche savoirs technologiques 4
- > Document 4

Même sensibilisés aux bonnes pratiques, les utilisateurs ne sont pas à l'abri d'une mauvaise manipulation ou d'une attaque malveillante. C'est pourquoi M. Brillat souhaite que vous lui proposiez un outil qui autorise ou non les connexions Internet vers certains sites. Il en a retenu deux, et vous demande votre recommandation.

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

- > Fiche savoirs technologiques 4
- > Document 5

Missions professionnelles

Dossier documentaire

Document 1 La sécurisation des connexions Internet

Voici des captures d'écrans de la configuration d'un poste de travail situé dans le bureau 4. Ce poste de travail est utilisé par les partenaires de la MSAP qui bénéficient d'une connexion Internet et d'un accès au réseau local pour la sauvegarde de leurs données.

Protection en temps réel

Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.

- ✖ La protection en temps réel est désactivée, ce qui rend votre appareil vulnérable.



Protection dans le cloud

Offre une protection renforcée et plus rapide grâce à l'accès aux données de protection les plus récentes dans le cloud. Fonctionne de manière optimale une fois la soumission automatique d'échantillons activée.



Notifications de protection contre les virus et menaces

Recevoir des notifications à caractère informatif



- Activités récentes et résultats d'analyse
- Des menaces ont été détectées, mais aucune action immédiate n'est nécessaire
- Les fichiers ou les activités sont bloqués

[Paramètres de protection contre les virus et menaces](#)

Document 2 La sécurisation des connexions aux réseaux et des applications

Voici une capture d'écran de la configuration d'un poste de travail situé dans la salle multimédia. Ce poste de travail est utilisé par les partenaires de la MSAP lors de formations professionnelles, mais aussi par les utilisateurs du public lors des créneaux en accès libre.

Connexions entrantes

Bloque les connexions entrantes sur un réseau privé.

- Bloque toutes les connexions entrantes, y compris celles de la liste des applications autorisées.



Contrôle des applications et du navigateur

Protection d'applications et sécurité en ligne.

Vérifier les applications et les fichiers

Le filtre Windows Defender SmartScreen aide à protéger votre appareil en recherchant les applications et les fichiers non reconnus à partir d'Internet.

- ⚠ La fonctionnalité Vérifier les applications et les fichiers est désactivée, ce qui rend votre appareil vulnérable. [Ignorer](#)

- Refuser
- Avertir
- Désactivé

Document 3

La configuration système d'un poste de travail nomade

Voici une capture d'écran de la configuration d'un ordinateur portable d'un partenaire utilisé en réseau avec le SI de la MSAP.



Document 4

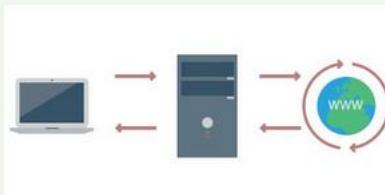
Les outils de sécurisation d'un poste de travail

Voici la liste des outils potentiellement utilisables au sein du télécentre de la MSAP.



Document 5

Les deux outils retenus par M. Brillat



Proxy Switcher

Un **proxy** est un serveur vers lequel tout le trafic Web est aiguillé. Il contient une **blacklist** qui bloque automatiquement la connexion à certains sites (*Accept* ou *Deny*). Ce serveur peut également être configuré pour appliquer des règles sur d'autres protocoles, comme FTP par exemple.

OpenDNS

OpenDNS Home Internet Security

OpenDNS Home Internet Security permet de bloquer certains contenus provenant d'Internet. En se connectant à un compte et en bloquant des catégories entières de contenus, à configurer ou à choisir selon ses besoins, on peut sécuriser les appareils connectés au réseau.

➤ Voir lexique BTS SIO, p. 221

Travaux en laboratoire informatique

1 Informer les utilisateurs sur les risques et promouvoir les bons usages à adopter



› Fiche savoirs technologiques 4

M. Brillat souhaite réaliser un audit sur la sécurité des identifiants de connexion pour s'assurer que la sensibilisation des utilisateurs a été efficace. Pour cela, il décide de faire réaliser des tests d'usurpation des éléments de connexion.

Pour réaliser cette tâche, vous devez disposer d'une machine virtuelle sous Windows 10 et d'une distribution Kali Linux (Free 2019, par exemple).

ÉTAPE 1 Préparation des tests

Plusieurs étapes sont préalables à la réalisation des tests : préparer les différents environnements de tests, récupérer la base **SAM** (*Security Account Manager*, « gestionnaire des comptes de sécurité ») et la sauvegarder dans un fichier.

1. Présentez le type d'audit que vous allez réaliser auprès de la MSAP.
› Document 1
2. Préparez la machine virtuelle Windows de test en reprenant les éléments mentionnés dans le guide de configuration.
› Document 2
› Fiche méthode 3, p. 207
3. Configurez l'environnement de travail Kali et sauvegardez la partition Windows selon les différentes commandes indiquées.
› Document 3

ÉTAPE 2 Première réalisation des tests

Votre environnement de travail est maintenant prêt. Vous allez réaliser deux types de tests (« force brute » et « dictionnaire ») qui vous permettront de trouver ou non les identifiants et mots de passe de chaque compte. Le compte administrateur sera également testé par défaut.

4. Exécutez les différents tests proposés par l'outil John the ripper. Pour cela, appuyez-vous sur les indications détaillées fournies.
› Document 4
5. Notez les identifiants trouvés et tirez les conclusions qui en découlent.

ÉTAPE 3 Seconde réalisation des tests

6. Modifiez le mot de passe du compte Enedis afin de renforcer la sécurité de cette authentification.
7. Proposez, d'après vos observations, au moins un critère qui permette d'améliorer la sécurité des mots de passe.

› Voir lexique BTS SIO, p. 221

Document 1 L'audit et les tests de pénétration

White Hat	Grey Hat	Black Hat
		

Le pentesteur travaille en étroite collaboration avec le DSI et l'équipe technique du SI. Il dispose de l'ensemble des informations.

Le test sera réalisé au départ avec un nombre limité d'information. On se place par exemple dans la situation où l'on est un utilisateur du SI.

Le testeur se met réellement dans la peau d'un attaquant externe et commence son test d'intrusion en ayant le moins d'information possible sur la cible.

Document 2 Le guide de configuration de la machine virtuelle Windows de test

- ① Sur la machine virtuelle Windows 10, s'authentifier avec le compte administrateur pour créer deux comptes supplémentaires :
- ENEDIS, avec un mot de passe de moins de huit caractères alphanumériques (exemple : judo15) ;
 - MSA, avec un mot de passe de plus de huit caractères alphanumériques.

- ② Indiquer dans les paramétrages de la VM qu'au lancement de la machine virtuelle, le *boot* (démarrage) sera réalisé sur le lecteur de disque.
- ③ Choisir l'ISO de la machine virtuelle Kali comme support.

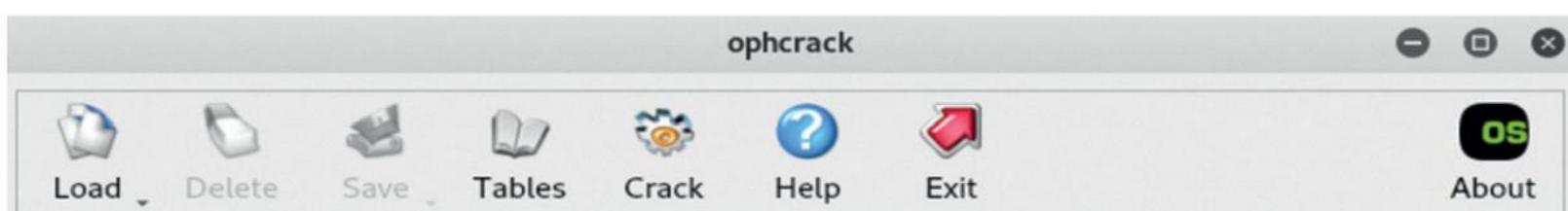
Document 3 La préparation de l'environnement Kali

Avant d'utiliser les différents outils proposés par la distribution Kali, il est nécessaire de réaliser plusieurs configurations :

- ① Modifier le clavier QWERTY en AZERTY avec la commande `setxkbmap fr`.
- ② Repérer la partition Windows avec la commande `fdisk -l`. Généralement, les différentes partitions sont représentées par le mot `sda` suivi d'un numéro. Il est probable que la partition la plus volumineuse soit celle recherchée. Noter le numéro de la partition, qui sera utile par la suite.
- ③ Monter la partition Windows identifiée précédemment dans Kali : `mount -t nfts /dev/sdax /mnt` (où `x` représente le numéro de la partition et `mnt` le dossier de destination).
- ④ Avant de commencer les tests, il convient de récupérer les identifiant et mot de passe des différents utilisateurs stockés dans la base SAM : elle contient les identifiants des comptes utilisateurs ainsi que leur mot de passe sous forme de haches - algorithme MD5.

Avec l'outil OPHCRACK :

- Bouton LOAD → Encrypted SAM → `mnt\Windows\System32\Config`



- Bouton SAVE → `\mnt\mdp.txt`

➤ Voir lexique BTS SIO, p. 221

Document 4 Tests à l'aide de l'outil John the Ripper

John the Ripper permet de tester la robustesse des mots de passe en utilisant plusieurs types d'attaques :

- à l'aide d'un dictionnaire ou Wordlist, qui correspond à un fichier avec un ensemble de mot de passe prédéfinis ;
- en testant l'ensemble des combinaisons possibles (en quelque sorte, une attaque en force brute).

Commandes	Explications
john --wordlist /mnt/mdp.txt	Test par dictionnaire Par défaut, le dictionnaire est password.lst
john --wordlist=NomDictionnaire.ext /mnt/mdp.txt	Il est possible de choisir un autre dictionnaire comme rockyou.txt
john --wordlist=NomDictionnaire.ext --rules /mnt/mdp.txt	Pour demander des combinaisons hybrides (exemple : a ↲ ↴ @)
john --incremental /mnt/mdp.txt	Pour un test incrémental
john --show /mnt/mdp.txt	Permet d'afficher les mots de passe récupérés

Remarques :

- Le dictionnaire **Rockyou.txt** se trouve dans le dossier **wordlists** : **/usr/share/wordlists**. Il doit être dézippé (gunzip).
- Le dictionnaire **password.lst** se trouve dans le dossier **john** : **/usr/share/john**. Ce dictionnaire peut être modifié par l'ajout de ses propres mots de passe. Dans le cas où les mots de passe ne sont pas connus, on peut deviner qu'un utilisateur aura utilisé le lieu + son nom + un chiffre pour constituer son mot de passe : msapMsa2. Utiliser pour cela la commande : **nano password.lst**.

```

GNU nano 2.8.7                               File: password.lst                         Modified

#!comment: This list has been compiled by Solar Designer of Openwall Project
#!comment: in 1996 through 2011. It is assumed to be in the public domain.
#!comment:
#!comment: This list is based on passwords most commonly seen on a set of Unix
#!comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!comment: (that is, more common passwords are listed first). It has been
#!comment: revised to also include common website passwords from public lists
#!comment: of "top N passwords" from major community website compromises that
#!comment: occurred in 2006 through 2010.
#!comment:
#!comment: Last update: 2011/11/20 (3546 entries)
#!comment:
#!comment: For more wordlists, see http://www.openwall.com/wordlists/
mspMsa2█
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
[ Read 3559 lines ]
^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos
^X Exit      ^R Read File   ^\ Replace    ^U Uncut Text  ^T To Spell   ^_ Go To Line

```

Travaux en laboratoire informatique

2

Identifier les menaces et mettre en œuvre les défenses appropriées

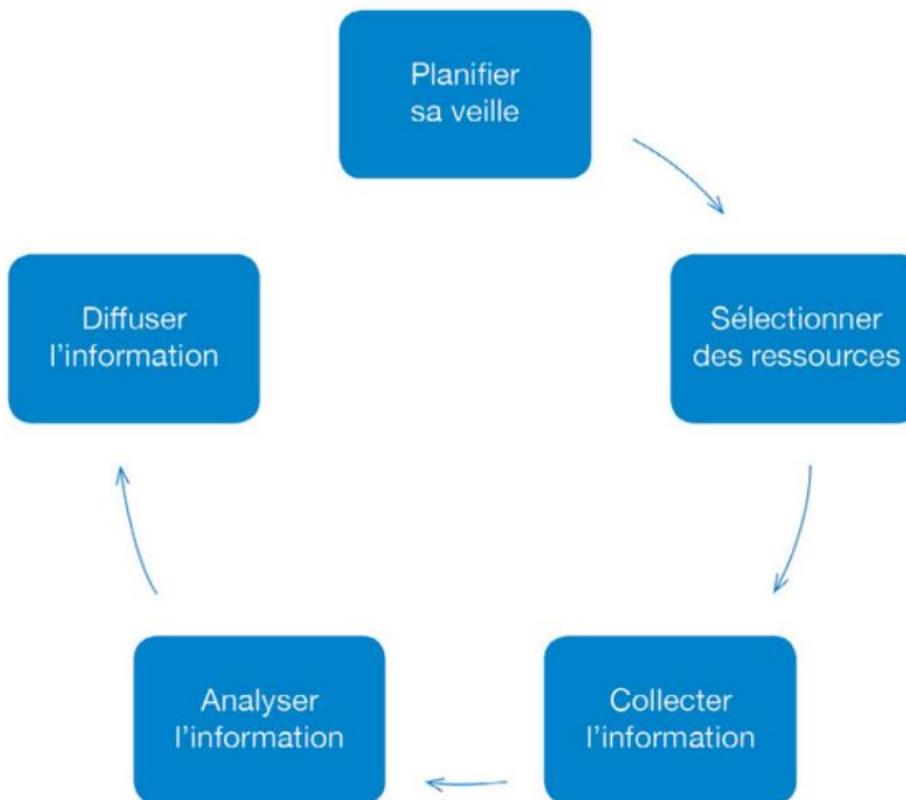


- Fiche savoirs technologiques 4
- Fiche méthode 1, p. 203

M. Brillat voudrait mettre en place une veille informationnelle sur les mises à jour et les correctifs logiciels liés au système Windows. Vous êtes en charge de la préparation de cette veille.

1. Définissez les objectifs de la veille informationnelle pour répondre à la demande de M. Brillat.
➤ Document 1
- M. Brillat a sélectionné un certain nombre de sources d'information, qu'il vous soumet. Cette liste n'est pas exhaustive. Elle ne contient pas l'ensemble des sources disponibles : elle est centrée sur les outils numériques.
➤ Document 2
2. Identifiez les différentes ressources numériques qui permettront de collecter les informations, en précisant si on peut les qualifier d'information de qualité. Pour cela, vous dresserez un tableau comparatif des différentes sources, en utilisant les critères suivants : rapidité d'accès, fiabilité, actualité et pertinence.
3. Comparez les trois outils de curation présentés dans le document 2, en vous aidant du tableau comparatif du document 3.
➤ Documents 3 et 4
➤ Tableau comparatif des outils de veille numérique : www.lienmini.fr/6988-401
4. Indiquez de quelle manière vous allez diffuser ces informations. Vous expliquerez les cibles ainsi que les canaux et les supports de communication utilisés.

Document 1 Les étapes de la veille informationnelle



Document 2 Des sources d'information sur Internet

Internet propose un grand nombre de possibilités pour accéder à de l'information. Voici une liste des principales sources :

- flux RSS, flux Atom ;
- newsletters, files d'actualité ;
- forums, communautés de pratique ;
- réseaux sociaux et réseaux sociaux d'entreprise ;
- système de syndication et de curation ;
- système d'alertes «push» et «pull».

Document 3 Des agrégateurs de flux Internet

M. Brillat a retenu trois outils de curation et de syndication de l'information.

**Document 4** Tableau comparatif des outils de veille numérique

Nom	Flux		Outils			Notifications		Avantages	Inconvénients	Web	Desktop	Mobile
	RSS	ATOM	Newsletters	Forums	Communauté	Réseau Social	Push					

➤ Voir lexique BTS SIO, p. 221

Fiche savoirs technologiques 4

La sécurité des terminaux utilisateurs et de leurs données

I

Définition

Sécuriser un terminal utilisateur et ses données implique de :

- réaliser des configurations système qui permettent de se protéger des attaques ;
- installer des applications et des matériels qui empêchent toute intrusion ;
- définir avec les utilisateurs les bonnes pratiques à adopter.

II

La configuration du système : quelques règles à respecter

Système d'exploitation	<ul style="list-style-type: none"> – Configurer les mises à jour automatiques – Installer les correctifs et les patchs
Applications	<ul style="list-style-type: none"> – Autoriser les applications vérifiées (signature) – Isoler les applications obsolètes – Interdire les téléchargements de sources inconnues – Limiter les modules optionnelles
Exécution automatique	Désactiver les ports et lecteurs
Boot sur périphériques externes	Désactiver le <i>boot</i> et insérer un mot de passe

III

Les applications et matériels spécifiques

Antivirus	Logiciel chargé de détecter et de stopper les <i>malwares</i> connus : virus, vers, <i>keylogger</i> , chevaux de Troie, etc. Il fonctionne avec une base de données qui contient les signatures des <i>malware</i> connus. Exemples : Bitdefender, Avast, Norton, Kaspersky.
Antispam	Le <i>spam</i> (ou courriel indésirable, ou pourriel) est une communication électronique non sollicitée. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. Exemples : Altospam, Postbox, McAfee.
Pare-feu (firewall)	Il inspecte les paquets réseaux entrants et sortants et implémente un mécanisme de filtrage basé sur des règles. Il ne transmet pas les paquets qui ne les respectent pas. On distingue les pare-feux matériels (pour un réseau) et les pare-feux logiciels (pour un poste de travail). Exemples : Sophos, Stormshield, ZoneAlarm.
Coffre-fort numérique (ou portefeuille de mots de passe)	Il permet de centraliser ses mots de passe en les protégeant par un seul mot de passe fort. Exemples : KeyPass ou 1Password.
Système d'authentification unique (en anglais <i>Single Sign-On</i> , SSO)	Un seul formulaire d'authentification permet d'accéder à l'ensemble des services de sa session utilisateur.
Mobile Device Management (« gestion des terminaux mobiles »)	Application qui permet la gestion d'une flotte d'appareils nomades. Son objectif est d'harmoniser les outils numériques avec des programmes et applications à jour et une sécurité correcte (présence d'un antivirus ou autre dispositif de sécurisation contre les <i>malwares</i>).

➤ Voir lexique BTS SIO, p. 221

IV

La promotion des bonnes pratiques

1. L'authentification

L'**authentification** permet de protéger le SI contre les attaques par dictionnaire, force brute, **table arc-en-ciel**.

Recommandations ANSSI pour obtenir une authentification forte							
R1	Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.						
R2	Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.)						
R3	Ne demandez jamais à un tiers de créer pour vous un mot de passe.						
R4	Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.						
R5	Renouvez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.						
R6	Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.						
R7	Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.						
R8	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.						
+ Choix du mot de passe :	Au moins 12 caractères de types différents, idéalement une passphrase (passe de phrase ou phrase secrète). Pour cela deux méthodes : <ul style="list-style-type: none"> • La méthode phonétique : « J'ai acheté huit CD pour cent euros cet après-midi » deviendra : ght8CD%E7am. • La méthode des premières lettres : la citation « un tient vaut mieux que deux tu l'auras » donnera : 1tvmQ2tl'A. 						
+ Authentification à double facteurs :	<table border="1"> <thead> <tr> <th>Quelque chose que je sais</th> <th>Quelque chose que je possède</th> <th>Quelque chose que je suis</th> </tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> • Mot de passe • Tracé de verrouillage </td> <td> <ul style="list-style-type: none"> • <i>One time password</i> : mot de passe temporaire Exemple : Token SafeNet </td> <td>Empreinte biométrique</td> </tr> </tbody> </table>	Quelque chose que je sais	Quelque chose que je possède	Quelque chose que je suis	<ul style="list-style-type: none"> • Mot de passe • Tracé de verrouillage 	<ul style="list-style-type: none"> • <i>One time password</i> : mot de passe temporaire Exemple : Token SafeNet 	Empreinte biométrique
Quelque chose que je sais	Quelque chose que je possède	Quelque chose que je suis					
<ul style="list-style-type: none"> • Mot de passe • Tracé de verrouillage 	<ul style="list-style-type: none"> • <i>One time password</i> : mot de passe temporaire Exemple : Token SafeNet 	Empreinte biométrique					

www.ssi.gouv.fr

2. Les bons usages sur Internet

Navigateurs	<ul style="list-style-type: none"> • Utiliser des protocoles SSL/TLS. • Effacer l'historique de navigations, les fichiers temporaires, les cookies.
Accès Internet	<p>Un proxy (serveur mandataire) est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour éviter les sites malveillants. Il permet :</p> <ul style="list-style-type: none"> • l'authentification des utilisateurs et la journalisation des requêtes ; • la mise en cache des pages consultées sur Internet afin d'accélérer les navigations, la mise en place de pare-feux ; • la sécurité par filtrage des paquets (entrant/sortant).
Courriels	<ul style="list-style-type: none"> • Désactiver l'exécution des liens hypertextes et l'affichage des images. • Être très vigilant avec les courriels dont les émetteurs sont inconnus et avec certains types de contenus. • Marquer les indésirables comme tels afin d'affiner la politique de détection des <i>spams</i>. • Si besoin, créer une adresse poubelle.

➤ Voir lexique BTS SIO, p. 221

I

La sécurité des équipements personnels des utilisateurs et de leurs usages

II

La structure d'une charte informatique

Généralement, la charte se présente sous la forme d'un document à portée juridique, dans lequel des instructions sont clairement définies.

1. Objectifs
<ul style="list-style-type: none"> • Les usages autorisés des ressources numériques • Les règles de sécurité en vigueur • Les mesures de contrôle prises par l'organisation
2. Définitions claires et précises
<ul style="list-style-type: none"> • Définition des termes clés pour éviter les interprétations divergentes <p> Exemple : définition du terme authentification</p>
3. Objet et portée
<ul style="list-style-type: none"> • Sur quoi la charte porte-t-elle (droits et devoirs des utilisateurs) ? <p> Exemple : obligation de longueur du mot de passe</p> <ul style="list-style-type: none"> • À qui est-elle destinée ?
4. Usages
<ul style="list-style-type: none"> • Les moyens informatiques et les outils numériques mis à disposition • Les règles et les pratiques autorisées • Les besoins auxquels doit répondre le système d'information
5. Devoirs des utilisateurs
<ul style="list-style-type: none"> • Bon sens dans les pratiques • Respect d'obligations techniques spécifiques
6. Les mesures de contrôle
<ul style="list-style-type: none"> • Liste des mesures de contrôle • Conditions dans lesquelles elles sont mises en œuvre
7. Sanctions
<ul style="list-style-type: none"> • Échelle de sanctions disciplinaires (proportionnelle à la gravité) • Sanctions civiles et pénales
8. Opposabilité de la charte
<ul style="list-style-type: none"> • Acceptation écrite par les utilisateurs • Annexion au règlement intérieur • Annexion au contrat d'entreprise et au contrat des prestataires



III

Le cadre juridique de la charte

La charte informatique doit être portée à la connaissance des salariés. Pour cela, l'employeur peut la présenter par voie d'affichage au sein de l'entreprise ou en remettre un exemplaire à chacun des salariés. La charte informatique s'applique à l'ensemble des utilisateurs du SI, quel que soit leur statut.

Ce document peut être opposable aux salariés de l'entreprise s'il est annexé à un règlement intérieur (l'employeur n'a pas obligation de faire signer la charte) ou au contrat de travail. La date d'entrée en vigueur de la charte doit être indiquée explicitement. Si elle est postérieure à un contrat de travail, un avenant devra être établi.

L'organisation peut imposer un droit de regard et de contrôle sur les pratiques des utilisateurs, par exemple en s'appuyant sur les fichiers journaux (*logs* des accès et modifications des fichiers), les connexions entrantes et sortantes à Internet et à la messagerie électronique, les appels téléphoniques, etc.

IV

Le cas particulier du nomadisme

L'organisation du travail dans les entreprises est aujourd'hui bouleversée par l'avènement de nouvelles habitudes de travail liées à l'apparition du BYOD, du COPE et du CYOD :

BYOD <i>Bring Your Own Device</i>	COPE <i>Corporate Owned Personnaly Enabled</i>	CYOD <i>Choose Your Own Device</i>
L'employeur autorise l'utilisation des équipements privés pour exercer les missions professionnelles.	L'entreprise fournit des équipements nomades et réalise la configuration.	Le salarié choisit son matériel mais sa configuration reste à la charge de l'employeur.

Ces nouvelles habitudes de travail doivent être prises en compte dans la rédaction de la charte informatique. En effet, elles impliquent et génèrent des contraintes supplémentaires. La **CNIL** formule des recommandations, notamment pour la protection des données personnelles.

La responsabilité de l'employeur joue également lorsque les données de l'entreprise sont stockées dans le matériel informatique personnel du salarié. L'employeur doit donc prendre les mesures nécessaires contre les risques relatifs à la **confidentialité** des données, aux intrusions et aux virus, et les mentionner dans la charte informatique.

Entre autres, il pourra spécifier :

- les appareils éligibles au BYOD ;
- les conditions d'utilisation de ces appareils ;
- les applications utilisables via un matériel personnel ;
- les documents accessibles par le biais d'un appareil personnel, etc.

1 QCM



Retrouvez ce QCM
en version interactive
www.lienmini.fr/6988-402

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 annexation au règlement intérieur.
- par annexation 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 Analyser un outil de protection numérique



› Fiche savoirs technologiques 4

Situation



Cyber'Ops, situé à Lyon, est un cybercafé accueillant principalement une clientèle d'adolescents. M. Archi, le gérant, souhaite installer un outil qui pourrait sécuriser les équipements et les usages des clients en contrôlant les connexions Internet. En effet, les sites sensibles, comme les sites pornographiques, à caractère discriminatoire ou encore religieux, ne doivent pas pouvoir être consultés.

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.

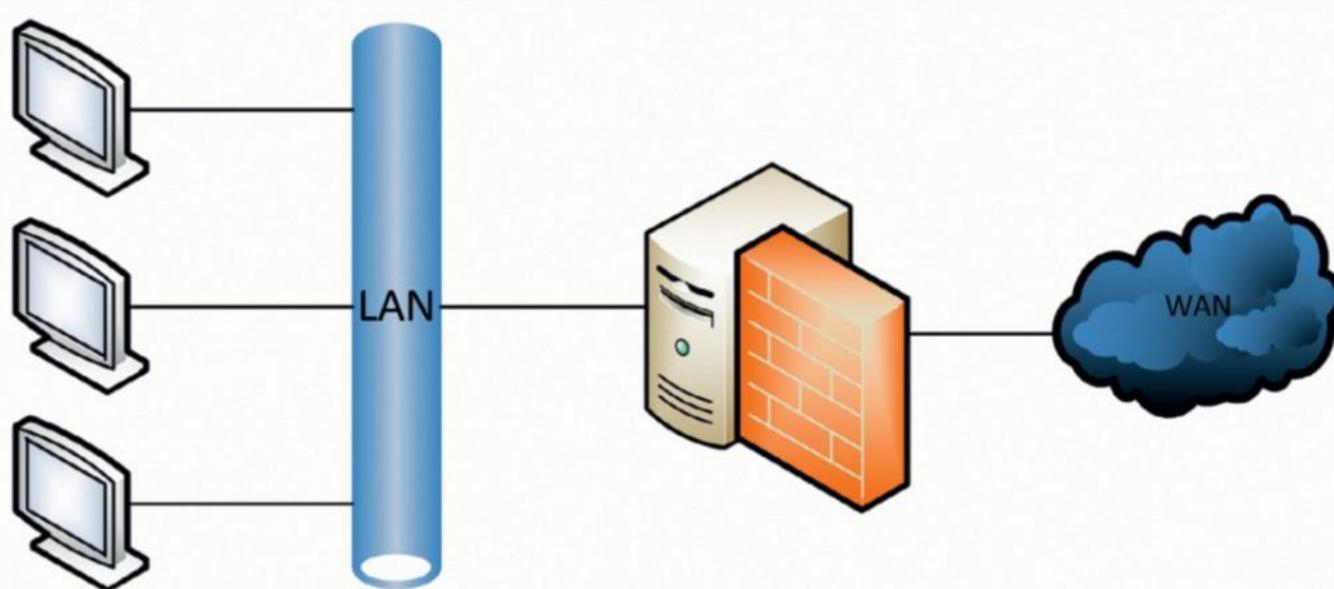
2 Expliquez de quelle manière cet outil autorise ou non la demande de connexion à un site spécifique.

3 Les adolescents sont également tentés d'utiliser ce lieu anonyme pour réaliser des téléchargements illicites (musique en MP3, vidéos, etc.).

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

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

Annexe Outils de sécurisation



3 Développer une configuration système



➤ Fiche savoirs technologiques 4

Situation

M. Archi ne peut surveiller en permanence les pratiques des utilisateurs sur leurs postes de travail (par exemple, l'utilisation de supports USB). Il doit donc prendre des précautions pour empêcher des utilisations frauduleuses de ces périphériques. Il souhaiterait que ces différentes configurations puissent être opérationnelles automatiquement, sans intervention quotidienne de sa part.

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

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

L'intégrité de l'environnement des postes de travail repose également sur un système d'exploitation non obsolète et exécutant des applications toujours mises à jour, c'est-à-dire toujours en maintenance et sans faille de sécurité.

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

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

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

4 Promouvoir les bonnes pratiques



➤ Fiche savoirs technologiques 4

Situation

M. Onnier est professeur au lycée Ada Lovelace à Saint-Maurice. Il intervient dans les classes de BTS SIO. Quotidiennement, les étudiants utilisent les ressources du réseau informatique de l'établissement. M. Onnier souhaite rédiger un guide des bonnes pratiques afin d'encadrer les usages de ses étudiants et, ainsi, les responsabiliser.



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.

- Guide de l'hygiène informatique : www.lienmini.fr/6988-403
- Guide des mots de passe : www.lienmini.fr/6988-404

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

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

...

Les étudiants seront souvent amenés à utiliser des identifiants de connexion sur des navigateurs Internet ou des logiciels spécifiques lors de leurs différents travaux.

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

M. Onnier propose à ses étudiants d'utiliser des machines virtuelles sous Windows 10 lors de leurs activités. Il vous demande d'étudier les options de sécurité locales proposées par ce système d'exploitation.

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

M. Onnier vous demande de créer un compte intitulé « etudiant_sio » sur une machine virtuelle Windows 10 et de tester ces stratégies.

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

Annexe

Stratégie de sécurité locale

The screenshot shows the Windows Local Security Strategy interface. The left pane displays a tree view of security policies under 'Paramètres de sécurité'. The 'Stratégies de comptes' node is expanded, showing 'Stratégie de mot de passe' which is also expanded. The right pane lists various password strategy settings with their current values:

Stratégie	Paramètre de sécurité
Conserver l'historique des mots de passe	0 mots de passe mémori...
Durée de vie maximale du mot de passe	42 jours
Durée de vie minimale du mot de passe	0 jours
Enregistrer les mots de passe en utilisant un chiffrement	Désactivé
Le mot de passe doit respecter des exigences de complexité	Désactivé
Longueur minimale du mot de passe	0 caractère(s)

5 Gérer les mots de passe



› Fiche savoirs technologiques 4

Situation

M. Onnier est conscient qu'il peut être parfois fastidieux pour les étudiants de mémoriser tous les mots de passe qu'ils auront à utiliser durant leurs deux années de scolarité sur l'ensemble des connexions serveurs et matériel. C'est pourquoi il souhaite que vous lui proposiez une analyse de l'outil KeyPass.

› Site keepass.info : www.lienmini.fr/6988-405

1 Consultez le tutoriel sur l'utilisation de Keepass :

› Utiliser Keepass pour gérer ses mots de passe : www.lienmini.fr/6988-406

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

3 Testez les fonctionnalités de l'outil.

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

Sécuriser l'accès aux ressources et vérifier l'efficacité

COMPÉTENCES

- Gérer les accès et les priviléges appropriés
- Vérifier l'efficacité de la protection

SAVOIRS ASSOCIÉS

- Authentification, priviléges et habilitations des utilisateurs : principes et techniques
- Gestion des droits d'accès aux données : principes et techniques
- Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction physique et logique
- Obligations légales de notification en cas de faille de sécurité

Situation professionnelle

Le directeur de la MSAP, M. Brillat, est inquiet. Récemment, des données du partenaire Enedis – qui étaient stockées sur le serveur de fichiers – ont été rendues accessibles à d'autres utilisateurs, malgré les restrictions appliquées.

C'est pourquoi M. Hiram, responsable de la DSI, vous demande d'améliorer la gestion des sessions utilisateurs, ainsi que l'organisation des droits d'accès aux données.



➤ Voir présentation générale, p. 83

Missions professionnelles

1

Gérer les accès et les priviléges appropriés

Les collaborateurs de la MSAP peuvent accéder aux services applicatifs du SI, après **authentification**. Ils ont notamment la possibilité de stocker leurs données sur le serveur de fichiers mis à leur disposition. Pour cela, ils disposent chacun d'un répertoire personnel. Malgré cela, des pertes de données ont été constatées récemment. M. Brillat a besoin de savoir si la politique de sécurisation – basée sur un système d'**habilitation** et d'**attribution de priviléges** qui tient compte du rôle de chaque utilisateur du SI – est efficace.

Vous êtes chargé(e) d'effectuer un relevé d'informations en observant les différentes configurations administrées.



Travail à faire

Vous réalisez un diagnostic de la pertinence des différentes stratégies de sécurisation des accès aux données. Plus précisément, vous devrez, d'après vos observations, valider la politique d'**habilitation** et d'**attribution** des priviléges aux utilisateurs.

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

- **Documents 1 et 2**
- **Fiche savoirs technologiques 5**

Vos observations ont permis de mettre en évidence des failles dans les habilitations accordées aux utilisateurs du télécentre. Avant de proposer des solutions, vous décidez de vous intéresser à présent aux droits d'accès accordés pour les partages du serveur de fichiers.

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

- **Documents 3 et 4**
- **Fiche savoirs technologiques 6**

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

- **Document 4**
- **Fiche savoirs technologiques 6**

Un des axes de votre mission consiste à proposer des solutions à M. Brillat pour garantir un contrôle efficace de l'accès aux données. Pour cela, vous devez lui indiquer quelles sont les bonnes configurations à effectuer sur les différents éléments qui constituent le SI de la MSAP.

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

- **Document 5**
- **Fiches savoirs technologiques 5, 6 et 7**

➤ Voir lexique BTS SIO, p. 221

Dossier documentaire

Document 1 L'authentification des utilisateurs et l'accès aux données

Les utilisateurs ne disposent pas de comptes locaux. Ils ne peuvent donc pas se connecter directement à une machine physique. Pour ouvrir une session, ils doivent s'identifier auprès de l'*Active Directory* (avec un identifiant et un mot de passe). Seul l'administrateur réseau, M. Jivon, possède un compte administrateur pour l'ensemble du parc informatique.

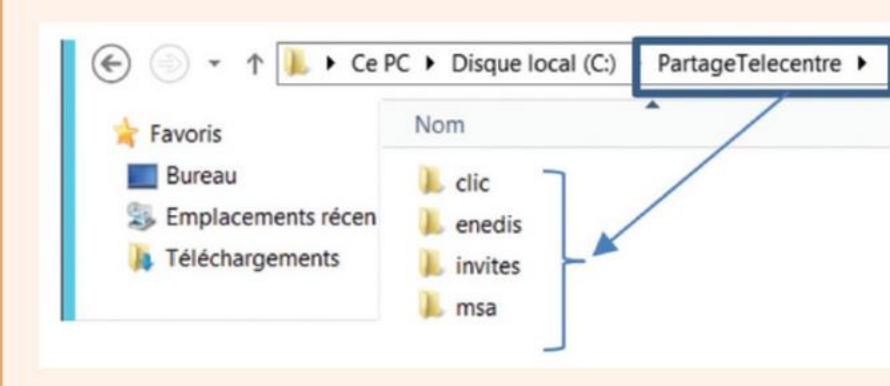
Gestion de l'ordinateur (local)	Nom	Nom complet	Description
Outils système	Administrateur		Compte d'utilisateur d'administrat...
Planificateur de tâches	DefaultAccount		Compte utilisateur géré par le syst...
Observateur d'événements	Invité		Compte d'utilisateur invité
Dossiers partagés	JIVON		
Utilisateurs et groupes			
Utilisateurs			
Groupes			

Document 2 Les priviléges des utilisateurs du télécentre

Tous les utilisateurs de la MSAP appartiennent à un groupe qui leur donne des priviléges au sein du domaine. Parfois, un groupe appartient à un groupe «parent» plus large, dont il hérite des priviléges.



Document 3 Présentation du serveur de fichier

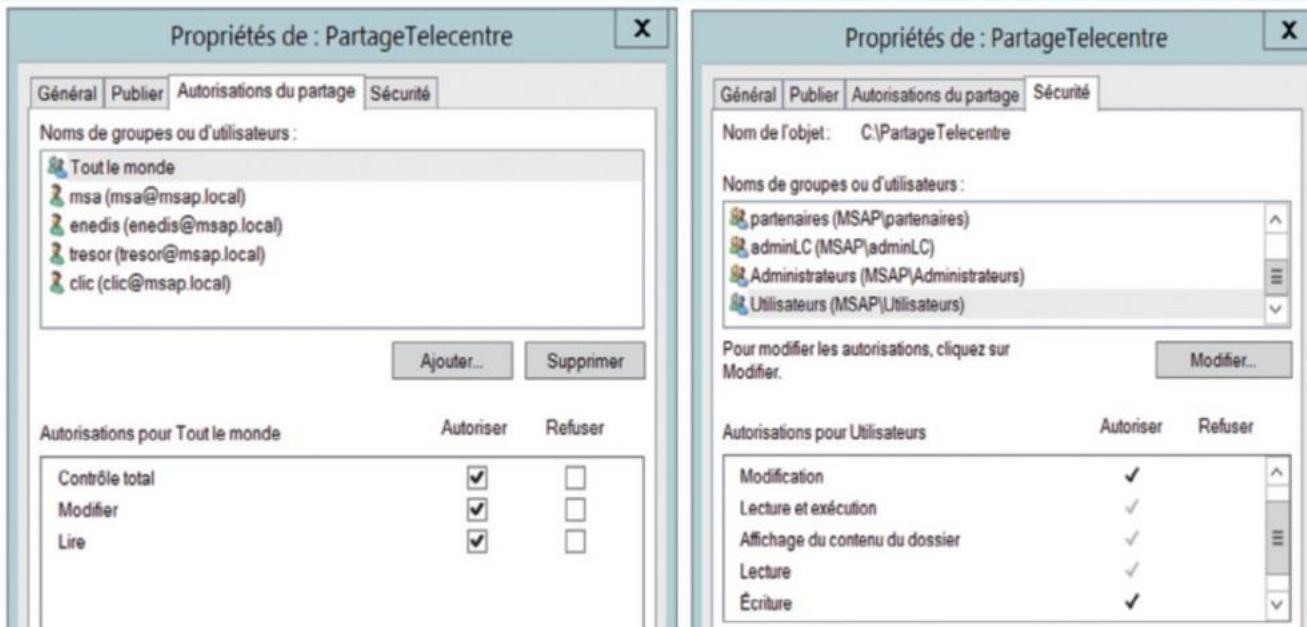


Le serveur de fichiers représente la même machine physique que l'*Active Directory*. Sur celui-ci, chaque partenaire dispose d'un dossier à son nom pour stocker ses données.

➤ Voir lexique BTS SIO, p. 221

Missions professionnelles

Document 4 Les autorisations et les accréditations accordées sur le dossier « PartageTelecentre »

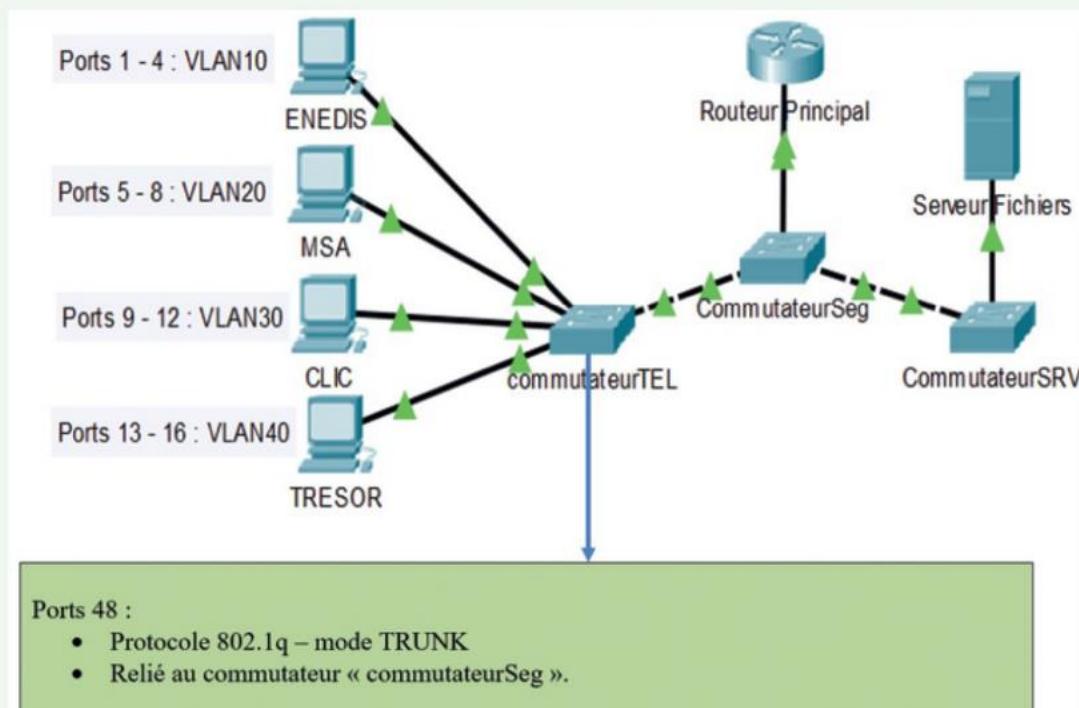


Document 5 La segmentation physique et logique de l'infrastructure du SI

• Le commutateur

Un **commutateur supplémentaire** (commutateurSeg) est intégré, sur lequel seront reliés tous les commutateurs du **LAN** de la MSAP. Celui-ci sera connecté directement au **routeur principal**.

Le schéma ci-contre présente le commutateur « commutateurTEL », sur lequel sont connectés tous les postes de travail du télécentre.



Sur les autres commutateurs, différents **VLANs** sont également configurés pour segmenter le réseau local. Le serveur de fichiers appartient au VLAN 100 (sur le commutateurSRV). Chaque VLAN possède son propre sous-réseau IP avec, comme valeur sur le troisième octet, le numéro de VLAN.

Exemple :

VLAN 10 pour le VLAN ENEDIS : 192.168.10.0 /24

• Le routeur principal

Des règles de filtrages (Access List) seront configurées sur le routeur principal.

Exemple :

« **le réseau 192.168.0.0 de masque /24 est autorisé à communiquer avec le réseau 192.168.100.0 de masque /24** ».

Sur un routeur Cisco, cette phrase se traduirait par la commande suivante :

Permit 192.168.0.0 0.0.255.255 192.168.100.0 0.0.0.255.

Pour qu'un réseau ne soit pas autorisé à communiquer avec un autre réseau, on utiliserait le terme **deny** dans la commande précédente à la place de **permit**.

➤ Voir lexique BTS SIO, p. 221

Missions professionnelles

2

Vérifier l'efficacité de la protection

M. Brillat a pris en compte vos préconisations et a chargé M. Jivon de les mettre en œuvre. Il souhaite à présent savoir si ces nouvelles configurations permettent réellement d'apporter une meilleure sécurité des données. Il vous demande de lui fournir une documentation lui permettant d'attester l'efficacité des protections mises en place.



Travail à faire

Vous avez réalisé une première phase de test pour vérifier que les différentes évolutions apportées au SI contribuent à maintenir la sécurité des données. Vous devez maintenant vérifier la pertinence des modifications effectuées en termes d'habilitations et d'autorisations.

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

- **Documents 1 et 2**
- **Fiches savoirs technologiques 6 et 7**

Votre diagnostic montre une réelle pertinence des configurations apportées aux SI. Cependant, il vous paraît judicieux de les renforcer.

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

- **Documents 3 et 4**
- **Fiche savoirs technologiques 6**

Votre deuxième phase de tests concerne la pertinence des modifications que vous avez apportées à l'infrastructure physique et logique du réseau de la MSAP. L'objectif de cette segmentation était d'empêcher l'ensemble des partenaires (identifiés par des VLANs et des sous-réseaux IP) de communiquer directement entre eux, tout en maintenant l'accès au serveur de fichiers.

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

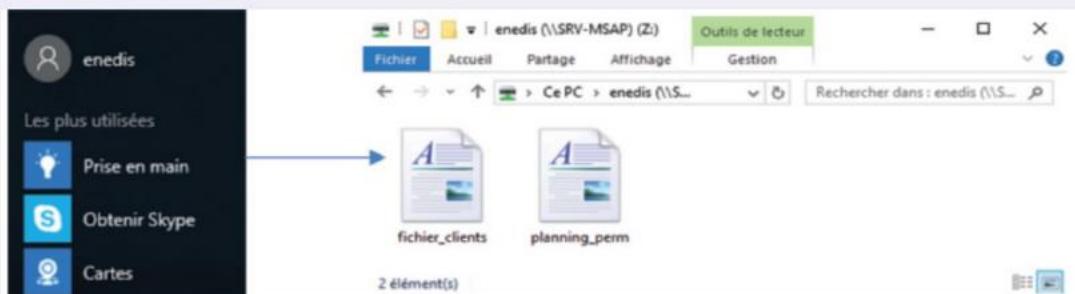
- **Documents 5 à 7**
- **Fiche savoirs technologiques 7**

Missions professionnelles

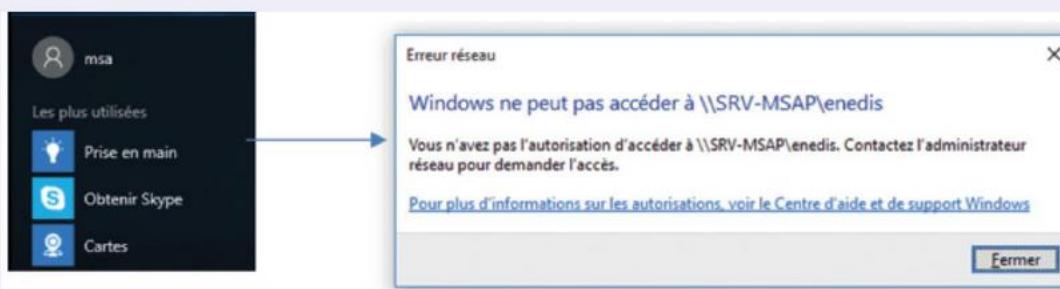
Document 1 Les tests sur les priviléges accordés pour chaque utilisateur

Vous devez accéder aux données figurant dans le dossier Enedis sur le serveur de fichiers. La connexion se fait d'abord avec le compte Enedis, puis avec le compte MSA.

- Connexion avec le compte Enedis



- Connexion avec le compte MSA



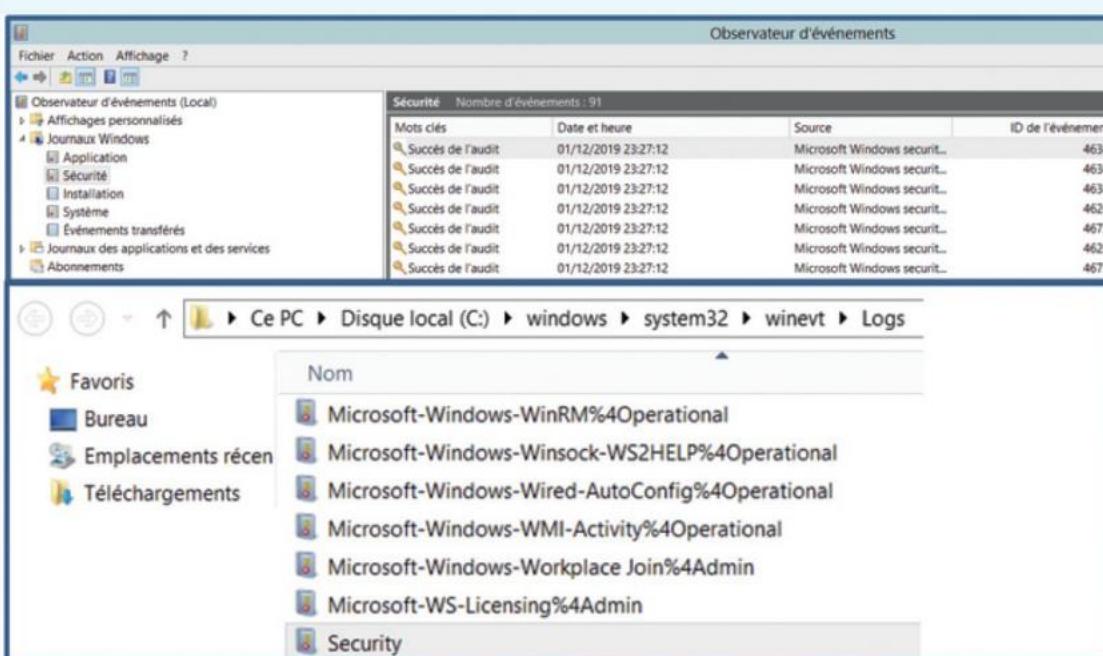
Document 2 L'installation d'applications

Vous êtes connecté(e) avec le compte Enedis et vous souhaitez installer l'application PuTTY (qui permet une connexion distante sur un matériel d'interconnexion) sur votre poste de travail.



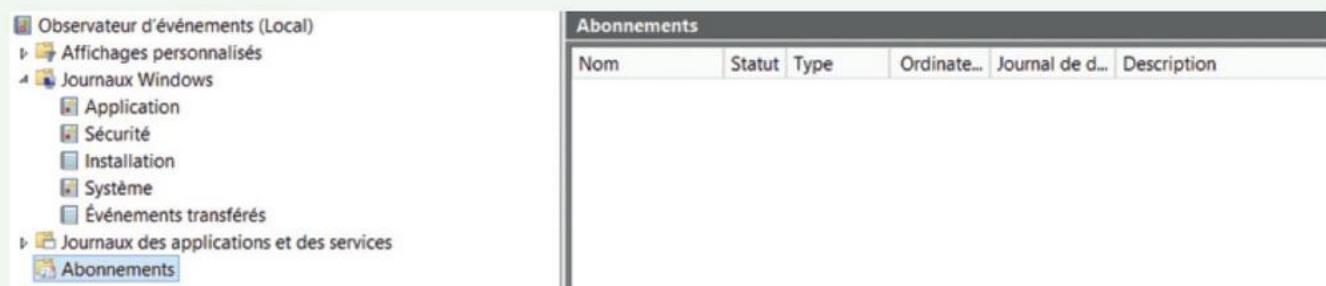
Document 3 La configuration des postes de travail

Vous avez lancé la commande **eventvwr.msc** sur les différents postes de travail pour connaître la configuration en termes de suivi des logs. La fenêtre ci-dessous montre le résultat de cette opération :



Document 4 Le serveur d'administration utilisé par M. Jivon

Vous avez effectué la même commande sur le serveur d'administration de M. Jivon mais, cette fois, vous vous êtes intéressé(e) au dossier Abonnements, qui contient le suivi des logs des postes du réseau local.



Document 5 Un extrait de la configuration du matériel d'interconnexion

• Le commutateur TEL

VLAN	Name	Status	Ports
1	default	active	Fa0/4, Fa0/5, Fa0/6 , Fa0/7 Fa0/8, Fa0/9, Fa0/10 , Fa0/11 Fa0/12, Fa0/13, Fa0/14 , Fa0/15 Fa0/16, Fa0/17, Fa0/18 , Fa0/19 Fa0/20, Fa0/21, Fa0/22 , Fa0/23 Fa0/24, Gig0/1, Gig0/2
10	enedis	active	Fa0/1
20	MA	active	Fa0/2

• Le routeur principal

```
"interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 102.168.10.254 255.255.255.0
 ip access-group ctsrv in
!
Interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.254 255.255.255.0
 ip access-group ctsrv in
!
ip access-list extended ctsrv
 permit ip 102.168.0.0 0.0.255.255 host
```

Document 6 Les tests avec la commande ping

Tests réalisés à partir d'un poste Enedis (192.168.10.1) vers un poste MSA (192.168.20.1) et vers le serveur de fichiers (192.168.100.1).

```
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data :

Reply from 192.168.10.254 : Destination host unreachable.

Ping statistics for 192.168.20.1 :
    Packets : Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Missions professionnelles

Layer 3: IP Header Src. IP: 192.168.20.1,
Dest. IP: 192.168.10.1 ICMP Message
Type: 8
Layer 2: Dot1q Header 00D0.D34C.9205
>> 0001.4231.EC01
Layer 1: Port GigabitEthernet0/0



1. The receiving port has an inbound traffic access-list with an ID of ctsrv. The device checks the packet against the access-list.
2. The packet matches the criteria of the following statement: deny ip any any. The packet is denied and dropped.

```
C:\>ping 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data :

Reply from 192.168.100.1 : bytes=32 time<1ms TTL=127

Ping statistics for 192.168.100.1 :
    Packets : Sent = 4, Received = 4, Lost = 0 (0% loss) ,
Approximate round trip times in milli-seconds :
    Minimum = 0ms,    Maximum = 0ms,    Average = 0ms
```

Document 7 La commande *tracert*

Commande réalisée à partir d'un poste Enedis vers un poste MSA puis vers le serveur de fichiers.

```
C:\>tracert 192.168.20.1

Tracing route to 192.168.20.1 over a maximum of 30 hops :

 1      2 ms      0 ms      0 ms      192.168.10.254
 2      0 ms      0 ms      0 ms      192.168.20.1

Trace complete.
```

```
C:\>tracert 192.168.100.1

Tracing route to 192.168.100.1 over a maximum of 30 hops :

 1      0 ms      0 ms      0 ms      192.168.20.254
 2      *          0 ms      0 ms      192.168.100.1

Trace complete.
```

1

Gérer les accès et les privilèges appropriés

➤ Fiches savoirs technologiques 5 et 6



Vous avez fait plusieurs recommandations à M. Brillat pour améliorer la sécurité des données au sein du SI de la MSAP. Vous avez notamment proposé la modification des différents éléments d'habilitation et des droits d'accès. M. Jivon est intervenu pour la réalisation de ces modifications. Cependant, dans un souci de disponibilité des données, il souhaiterait installer un second serveur de fichiers (à l'identique du premier) pour remplacer le premier en cas de dysfonctionnement ou de panne.

1. Préparez la machine virtuelle de tests (second serveur de fichiers) d'après les consignes.
 - Document 1
 - Fiche méthode 3, p. 207
2. Créez les différents partages en relevant les chemins d'accès qui servent à définir un lecteur réseau pour chaque compte.
 - Documents 2 et 3
3. Définissez les autorisations et les ACL (liste de contrôle d'accès) sur les partages en vous appuyant sur les recommandations données.
 - Documents 4 et 5
4. Réalisez les tests.
 - Document 6

Document 1 Consignes pour la préparation de la machine virtuelle de tests

1. Installer le rôle serveur de fichiers sur une machine virtuelle Windows 2012 R2.
2. Attribuer l'ensemble des privilèges au compte Administrateur.
3. Créer des comptes Enedis, MSA, CLIC et TRESOR en local sur le serveur à l'aide du compte Administrateur. Mot de passe pour chaque compte : **MSAPconnect1920**.
4. Valider la case à cocher « modifier le mot de passe à la première connexion » pour chaque compte.

Document 2 Informations sur les dossiers de partage

1. Création d'un dossier nommé « partages » à la racine du lecteur C du serveur de fichiers.
2. Création des différents dossiers de partage pour chaque utilisateur précédemment admis à l'intérieur du dossier « partages ». Chaque dossier de partage portera le même nom que le compte associé.

Document 3 Un exemple de partage sur un dossier

Le compte test et le dossier correspondant.



TESTS

\Desktop-579b371\tests

➤ Voir lexique BTS SIO, p. 221

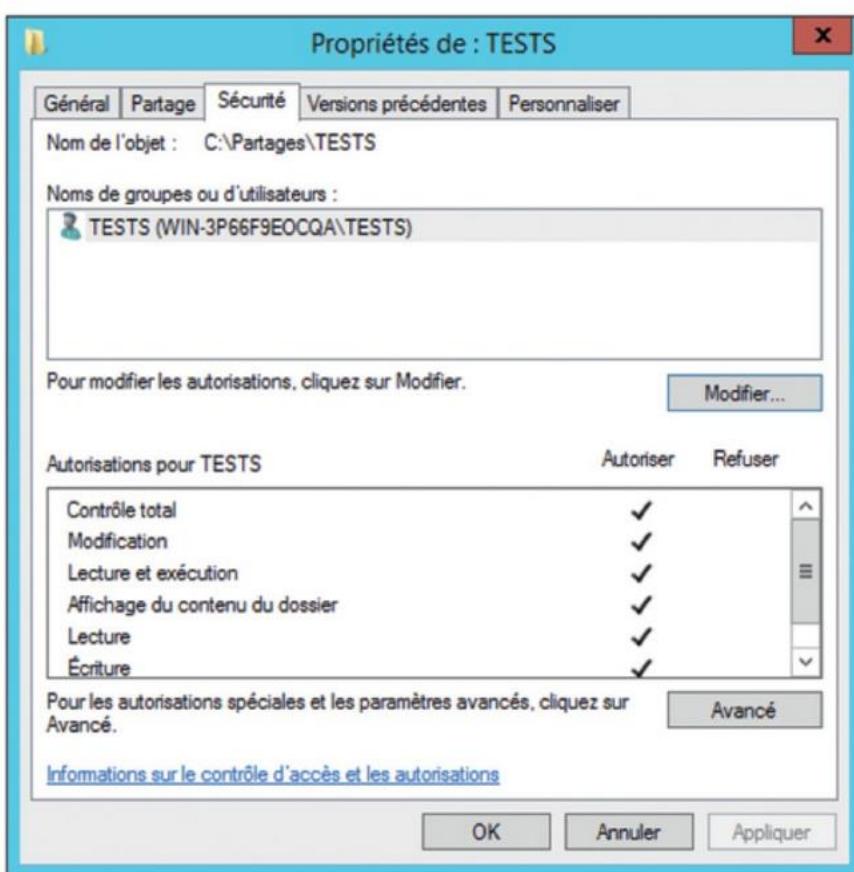
Document 4 Un exemple de définition d'une autorisation sur un partage

The left screenshot shows the Windows File Explorer context menu for a folder named 'TESTS'. It highlights the 'Partage de fichiers' (File sharing) option. Below it, a window titled 'Partage de fichiers' displays the message 'Choisir les utilisateurs pouvant accéder à votre dossier partagé' (Select the users who can access your shared folder). A search bar and a list of users ('Administrateurs' and 'TESTS') with their respective permission levels ('Propriétaire' and 'Lecture/écriture') are shown.

The right screenshot shows the 'Autorisations pour TESTS' (Permissions for TESTS) dialog box. It lists the user 'TESTS (WIN-3P66F9EOCQA\TESTS)' under 'Noms de groupes ou d'utilisateurs'. The 'Autorisations pour TESTS' table shows the following permissions:

Autorisations pour TESTS	Autoriser	Refuser
Contrôle total	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modifier	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lecture	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Document 5 Consignes pour la définition des ACL sur les partages



1. Créer l'accès au dossier (seul le compte portant le même nom que le dossier peut accéder au dossier).
2. Définir un contrôle total sur les données (on considère que les utilisateurs qui accèdent au partage sont les propriétaires des données).

Document 6 Tests à réaliser

• Test 1

- Connexion avec le compte Enedis.
- Définir le mot de passe de session. Celui-ci sera modifié par la suite.
- Créer un lecteur réseau avec le chemin de partage relevé précédemment (question 2).
- Ajouter un document dans le répertoire, le modifier, puis le supprimer.

• Test 2

- Se déconnecter du compte Enedis.
- Ouvrir une session avec le compte MSA.
- Créer un lecteur réseau avec le chemin de partage utilisé dans le test 1.
- Identifier le message d'erreur (le commenter).

2

Vérifier l'efficacité de la protection



- Fiche savoirs technologiques 7
- Fichier Packet Tracer : www.lienmini.fr/6988-501

Afin de suivre vos recommandations, M. Jivon a procédé à une segmentation physique et logique du réseau de la MSAP. L'ensemble du matériel est configuré, hormis le commutateurTEL et le routeur principal. Il vous demande donc d'effectuer les modifications adéquates en adaptant le fichier Packet Tracer fourni.

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

- Document 1

2. Configurez le commutateurTEL pour intégrer les VLAN.

- Documents 2 et 3

Avec l'ajout du commutateurTEL, la segmentation physique du réseau nécessite également des modifications sur le routeur principal. Vous devez configurer celui-ci.

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

- Document 4

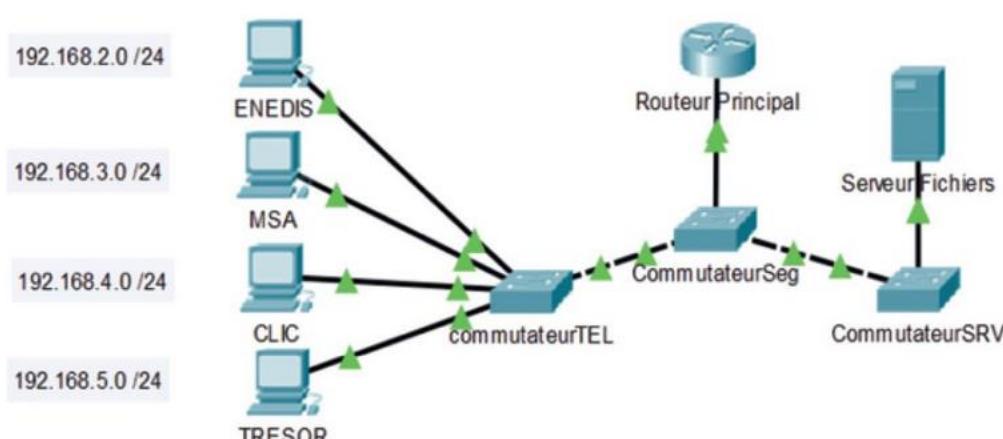
Vous avez terminé la configuration des différents matériels d'interconnexion de la nouvelle infrastructure du réseau de la MSAP. Vous devez à présent vérifier le bon fonctionnement de celle-ci.

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

- Document 5

Document 1 Le schéma de l'infrastructure réseau de la MSAP

Création et configuration de la nouvelle infrastructure réseau de la MSAP avec un outil de simulation réseau, comme Cisco Packet Tracer.



Précisions :

Poste ENEDIS relié au port 2 du commutateurTEL.
Poste MSA relié au port 3 du commutateurTEL.
Poste CLIC relié au port 4 du commutateurTEL.
Poste TRESOR relié au port 5 du commutateurTEL.
Serveur de fichiers relié au port 23 du commutateurSeg.
Le commutateur est relié à l'interface GigabitEthernet 0/1 du routeur par son port Fa 0/24.

Adresse IP des postes :

ENEDIS 192.168.2.1

MSA 192.168.3.1

CLIC 192.168.4.1

TRESOR 192.168.5.1

Serveur de fichiers : 192.168.100.100

Document 2 Informations concernant les VLANs à configurer

ENEDIS : VLAN 20
CLIC : VLAN 40

MSA : VLAN 30
TRESOR : VLAN 50

Le port 1 reste dans le VLAN 1 ; il est considéré comme VLAN de management par la suite.

Document 3 Commandes de configuration d'un commutateur

- Pour nommer un commutateur :

Commutateur (config)#hostname NOM

- Pour définir le mot de passe dans le mode « privilégié » :

Commutateur (config)#enable secret MotdePasse

- Pour configurer les VLAN :

Commutateur > enable

Commutateur #conf t

Commutateur (config)#vlan 10

Commutateur (config-vlan)#name ENEDIS

Commutateur (config)# int fat 0/2

Commutateur (config-if)#switchport access vlan 10

Document 4 La configuration du routeur principal

Le commutateur est relié au routeur par une interface physique, mais plusieurs sous-réseaux logiques doivent pouvoir accéder à leur passerelle. C'est pourquoi il faut créer des interfaces virtuelles sur cette interface physique.

Exemple de commande :

```
RouteurPrincipal #conf t
RouteurPrincipal (config)#int gigabitEthernet 0/1.2 //2 représente le numéro de vlan
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
RouteurPrincipal (config-subif)#exit
```

Par la suite, comme présenté précédemment, il convient de configurer les *Access lists* pour interdire la communication entre les différents réseaux et autoriser la communication avec le serveur de fichiers. Ce travail sera à réaliser lors d'une prochaine mission.

Document 5 Les tests de validation de l'infrastructure réseau de la MSAP

- Vérifier que les postes passent par le routeur pour émettre des trames à destination d'un autre VLAN,
- Vérifier que l'ensemble des VLAN accède au serveur de fichiers.
- Réaliser des copies d'écran des différents tests en mettant en évidence les commandes utilisées.

Fiche savoirs technologiques 5

Les authentifications, privilèges et habilitations des utilisateurs

I

Les principes de l'authentification et de l'habilitation

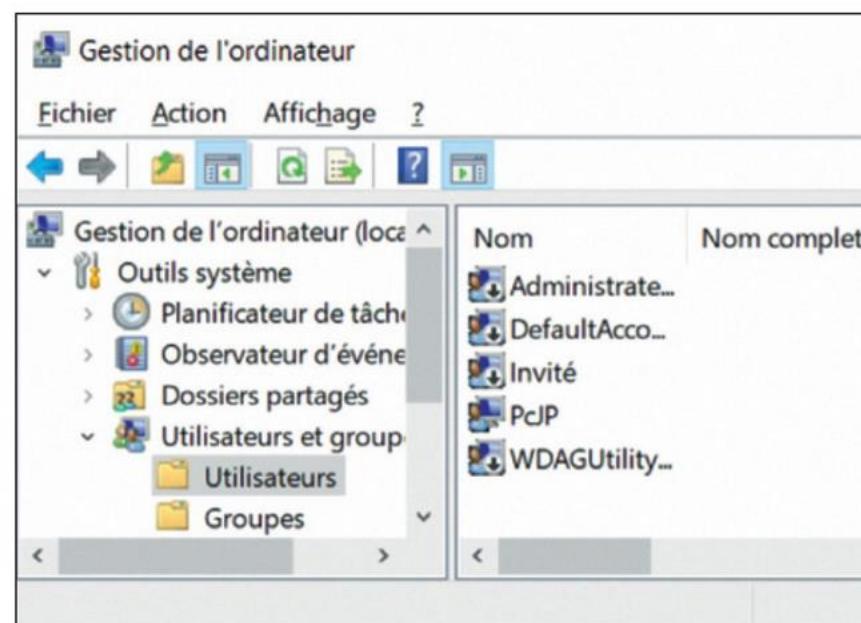
Authentification	Habilitation
<p>Processus qui permet de vérifier si l'utilisateur est bien celui qu'il prétend être.</p> <ul style="list-style-type: none"> • Elle permet de vérifier et de prouver l'identité d'un utilisateur qui veut ouvrir une session dans un SI, et de lui accorder les droits d'accès inhérents à son compte. • Elle s'appuie sur l'utilisation d'un identifiant (<i>login</i>) et d'un mot de passe (<i>password</i>). • Elle repose sur un compte utilisateur local ou un compte utilisateur sur un gestionnaire de domaine, comme Active Directory. 	<p>Processus qui permet de savoir si un utilisateur a accès à une ressource ou non.</p> <ul style="list-style-type: none"> • Elle inclut l'autorisation, l'accréditation, les droits d'accès ou encore le contrôle d'accès. • Elle donne la permission à un utilisateur de réaliser des actions sur des ressources du SI : droit de consultation, droit de création, droit de modification, droit de suppression, etc. • Elle dépend des priviléges accordés. Le privilège est la délégation d'autorité sur un fichier ou un dossier dans un SI.

II

Les techniques d'authentification

1. Le compte local

L'accès à un poste de travail s'effectue par des comptes utilisateurs. Ces comptes peuvent être nominatifs (chacun est associé à une seule personne) ou collectifs (des comptes sont associés à plusieurs personnes). Par défaut, le compte administrateur et le compte invité sont créés. L'ensemble des comptes locaux et des mots de passe sont stockés (sous forme d'empreintes numériques) dans la base **SAM** (Security Accounts Manager - %SystemRoot%\System32\Config\SAM).



2. Les comptes itinérants

Les authentifications centralisées sur un contrôleur de domaine s'effectuent grâce à l'annuaire **LDAP** (*Lightweight Directory Access Protocol*) et au protocole **Kerberos** (protocole réseau d'authentification reposant sur un chiffrement symétrique et un système de tickets).

➤ Voir lexique BTS SIO, p. 221

…>

III

Les techniques d'habilitations associées aux comptes utilisateurs

Ajuster les paramètres de l'ordinateur

Afficher par : Catégorie

Système et sécurité

- Consulter l'état de votre ordinateur
- Sauvegarder l'ordinateur
- Rechercher et résoudre des problèmes

Comptes et protection des utilisateurs

- Ajouter ou supprimer des comptes d'utilisateurs
- Configurer le contrôle parental pour un utilisateur

Les **comptes administrateurs** (ou superutilisateurs) possèdent les priviléges les plus élevés. Ils ont un contrôle total sur l'ensemble des ressources du SI. Ces comptes sont par ailleurs habilités à créer, modifier et supprimer d'autres comptes.

Les **comptes utilisateurs** n'ont pas la possibilité de réaliser des opérations privilégiées, ni de créer des comptes. Ils peuvent cependant configurer le système et installer certains logiciels.

Les **comptes invités** sont des comptes génériques aux droits très restreints. Ils ne peuvent pas installer des logiciels et n'ont pas accès aux répertoires contenant des informations sensibles. Chaque compte utilisateur appartient à un groupe d'utilisateurs qui définit, par défaut, ses droits d'accès ou priviléges.

IV

Les bonnes pratiques en matière d'authentification et d'habilitation

Authentification	Habilitation (valable pour l'ensemble des comptes)
Compte administrateur <ul style="list-style-type: none"> Utiliser des comptes d'administration dédiés et non partagés entre différents utilisateurs : l'administrateur doit disposer de plusieurs comptes d'administration distincts selon les tâches qu'il doit réaliser. Protéger (confidentialité et intégrité) l'accès aux annuaires des comptes administrateurs. Ne pas autoriser l'ouverture de sessions de travail (activités qui ne sont pas de l'ordre de l'administration) sur des postes réservés aux actions d'administration. Attribuer des droits d'administration à des groupes plutôt qu'à des utilisateurs individuels. 	<ul style="list-style-type: none"> Respecter le principe « du besoin d'en connaître » : habilitations nécessaires à la réalisation des tâches inhérentes à l'activité de l'utilisateur. Respecter le principe « du moindre privilège » : mettre en place des habilitations strictement nécessaires aux activités liées à chaque compte. Ce principe ne doit pas être supérieur au « besoin d'en connaître ». Gérer efficacement les mobilités : éviter l'accumulation des habilitations (fonctions successivement occupées).
Compte utilisateur <ul style="list-style-type: none"> Doit être nominatif. Ne pas utiliser de comptes partagés entre plusieurs utilisateurs. Donner accès seulement aux données nécessaires aux activités et restreindre l'accès aux répertoires contenant des données sensibles. Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour. Ne pas donner accès aux disques et aux applications sensibles aux utilisateurs visiteurs. 	<ul style="list-style-type: none"> Réaliser une revue annuelle des habilitations afin d'identifier et de supprimer les comptes non utilisés ou qui n'ont plus lieu d'exister. Mettre en place des procédures d'attributions des habilitations à appliquer systématiquement à l'arrivée ainsi qu'au départ ou au changement d'affectation d'un utilisateur du SI. Définir des mesures permettant de restreindre et de contrôler l'attribution et l'utilisation des accès.

➤ Voir lexique BTS SIO, p. 221

Fiche savoirs technologiques 6

La gestion des droits d'accès aux données

Le contrôle d'accès précise qui (utilisateur) est autorisé à faire quoi (lectures, écritures, suppressions, modifications, etc.) sur quelles données.

I

Les principes de la gestion des droits d'accès aux données

Elle a pour but de limiter les actions qui peuvent être réalisées sur les données (fichiers et dossiers), l'utilisation des applications et la gestion du système.

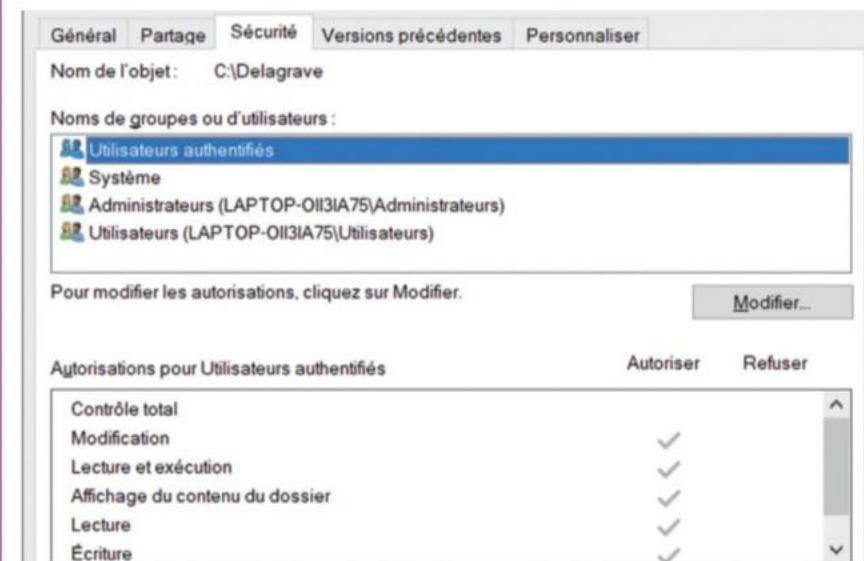
Le principe est de restreindre les priviléges des différents utilisateurs.

Exemple sous UNIX : la commande **ls -al** affiche les droits sur les fichiers et les répertoires, représentés par les lettres ci-dessous :

r - read	Lire un fichier/lister un répertoire	
w - write	Ajouter, supprimer, modifier un fichier dans un répertoire	
X - execute	Exécuter un fichier / traverser un répertoire	
Droits	Utilisateurs	Ressources concernées
-rwxr-x---	1 root	apple.exe
drw-r----	1 brows	Reports
-rw-rw-r--	1 darkness	gold.txt

La commande **chmod** munie des opérateurs **+, -, u,** permet de modifier et de changer les droits d'accès.

Exemple sous Windows : les droits d'accès s'appuient sur le **système de fichiers NTFS** pour pouvoir mettre en œuvre un modèle de moindre privilège grâce à des listes de contrôle d'accès (ACL). La gestion des autorisations se fait à partir de l'onglet « Sécurité » de chaque dossier ou fichier :



Les différents priviléges sont :

- l'accès au contenu du répertoire (Afficher le contenu du dossier) ;
- la lecture des fichiers, de leurs propriétés et de leurs répertoires (Lecture) ;
- l'exécution des programmes et des scripts (Lecture et exécution) ;
- l'écriture dans les fichiers et l'ajout des fichiers dans les répertoires (Écriture) ;
- l'affichage, la modification, la suppression des fichiers et répertoires (Modifier) ;
- tous les droits (Contrôle total) habituellement réservés à l'administrateur : modification, ajout, déplacement ou suppression des fichiers et répertoires ;
- la modification des paramètres des autorisations pour tous les autres utilisateurs.

➤ Voir lexique BTS SIO, p. 221

…>

II

Les outils de la gestion des droits d'accès aux données

Différents modèles de gestion des droits d'accès sont possibles au sein d'un système d'information, mais leur finalité est la même : ne permettre l'accès et la modification des données qu'aux personnes autorisées. Les deux principaux modèles sont :

DAC <i>(Discretionary Access Control)</i> Contrôle d'accès discrétionnaire	RBAC <i>(Role-Based Access Control)</i> Contrôle d'accès basé sur des rôles
<p>Le créateur d'une ressource est le propriétaire de celle-ci. Il fixe alors la politique de contrôle d'accès de cette ressource : il décide quel utilisateur peut réaliser quelle action.</p> <p>Exemple : En tant que propriétaire du fichier paie.xls, j'autorise uniquement Alice à lire le fichier.</p>	<p>Il convient de définir tout d'abord des rôles qui représentent un ensemble de priviléges. Les utilisateurs sont affectés à un rôle et héritent donc des droits inhérents à celui-ci.</p> <p>Exemple : Le rôle RH donne les droits d'accès en lecture et en écriture au fichier paie.xls. On attribue le rôle à Bob, qui pourra donc modifier le fichier.</p>
<p>Ce modèle de gestion est décentralisé. Il correspond à l'attribution de droits par un compte local sur un poste de travail.</p>	<p>Ce modèle de gestion est centralisé, comme dans un <i>Active Directory</i> où les utilisateurs appartiennent et héritent des groupes.</p>

III

La gestion dans le cadre d'un *Active Directory*

Dans un *Active Directory* (gestion centralisée des utilisateurs), des groupes de sécurité sont prédéfinis pour attribuer des droits particuliers aux différents comptes (utilisateurs) créés. Ci-dessous, un exemple de groupes présents dans l'*Active Directory* :

Administrateurs	Accès complet et illimité à l'ordinateur promu du domaine
Administrateur du domaine	Droits sur tous les objets du domaine et administration du domaine
Opérateurs de comptes	Création, modification et suppression des objets locaux
Utilisateurs du domaine	Groupe par défaut de tout nouvel utilisateur
Invité du domaine	Inclut le compte invité du domaine. Lorsque les membres de ce groupe se connectent, un profil de domaine est créé sur l'ordinateur

La sécurité des communications numériques

La sécurisation des communications (acheminements des données) dans un réseau local implique l'utilisation de protocoles spécifiques et la mise en œuvre d'infrastructures réseaux particulières pour segmenter (diviser) de façon logique et physique le réseau interne.

I

Le protocole de sécurisation des communications

Un protocole est un ensemble de règles à suivre pour établir une communication dans un réseau informatique. La communication peut être sécurisée en utilisant des protocoles spécifiques :

- le **protocole 802.1x** : c'est une solution standard de sécurisation des réseaux mise au point par l'IEEE (*Institute of Electrical and Electronics Engineers*, Institut des ingénieurs électriciens et électroniciens). Il s'appuie sur le protocole AAA (*Authentification, Authorization, Accounting/Auditing*), un modèle de sécurité qui a trois fonctions : authentification, autorisation et **traçabilité**. Il permet à un utilisateur souhaitant accéder à un réseau de s'authentifier grâce à un serveur central d'authentification ;
- le **protocole EAP** (*Extensible Authentication Protocol*) : il permet la demande d'autorisation de connexion au serveur (support universel permettant le transport de différentes méthodes d'authentifications) ;
- le **protocole SSH** (*Secure Shell*) : il permet d'administrer les matériels d'interconnexion, les administrateurs réseaux. Il impose un échange de clés secrètes de chiffrement en début de connexion.

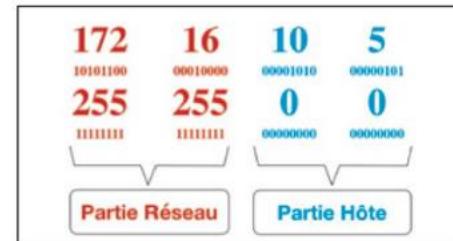
II

La segmentation et les restrictions logiques des réseaux

Segmenter un réseau permet de diviser celui-ci en plusieurs sous-réseaux et, ainsi, d'imposer des règles supplémentaires pour autoriser les communications.

1. Les sous-réseaux IP

Dans un réseau local, les hôtes sont identifiés par des adresses IPv4 privées constituées de 4 octets de 8 bits. Une adresse est composée d'une partie réseau, qui définit le réseau d'appartenance de l'hôte, et d'une partie hôte, qui identifie l'hôte dans son réseau. Tous les hôtes d'un même réseau peuvent communiquer entre eux : on parle de domaine de diffusion. Cependant, les hôtes appartenant à des réseaux différents ne peuvent pas s'échanger des informations directement : ils doivent utiliser une passerelle.



2. Les VLANs

Un VLAN (*Virtual Local Area Network*) décrit un réseau local virtuel. Son objectif est de regrouper de façon logique et indépendante un ensemble d'hôtes. Il permet de créer des domaines de diffusion gérés par les commutateurs indépendamment de l'emplacement géographique où se situe le nœud. On distingue trois types de VLANs :

- le **VLAN de niveau 1** : on affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est alors déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN ;
- le **VLAN de niveau 2** : on affecte manuellement chaque adresse MAC à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par son adresse MAC. L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation ;
- le **VLAN de niveau 3** : on affecte un protocole de niveau 3 ou de niveau supérieur à un VLAN. L'appartenance d'une carte réseau à un VLAN est alors déterminée par le protocole de niveau 3 ou supérieur qu'elle utilise.

➤ Voir lexique BTS SIO, p. 221



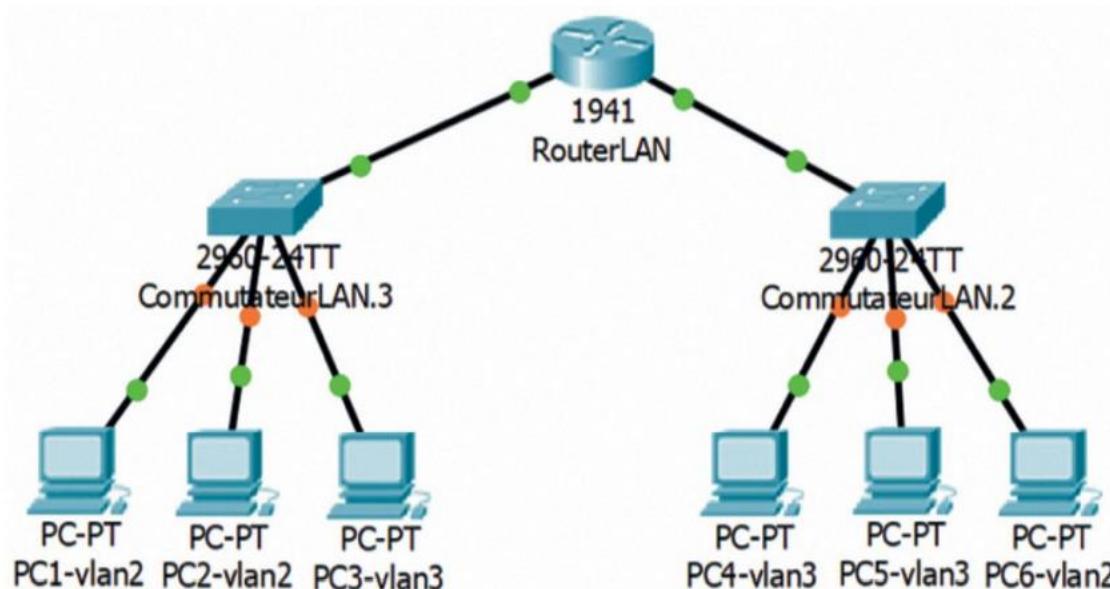
III

La segmentation et les restrictions physiques des réseaux

Un réseau informatique est constitué d'équipements d'interconnexion permettant de répartir de façon physique et logique (sous-réseau IP et VLANs) les différents hôtes du LAN.

1. Les commutateurs

Sans VLAN, un commutateur (*switch*, en anglais) considère que toutes ses interfaces sont dans le même LAN et le même domaine de diffusion. Avec la mise en place de VLANs, un commutateur place ses interfaces dans des sous-réseaux et domaines de diffusion différents. Un commutateur a alors plusieurs séparations logiques sur un même support physique.



Par défaut, sans configuration précise, les ports d'un commutateur sont dans le VLAN 1. L'administrateur réseau doit donc configurer chaque port du commutateur dans un VLAN particulier (par exemple, avec un commutateur Cisco : *Switch port mode acces vlan 2*). Pour permettre la communication entre des VLANs différents, il faut configurer un port en mode trunk (norme 802.1q) et relier ce port au routeur pour assurer le routage inter-VLAN.

2. Les routeurs

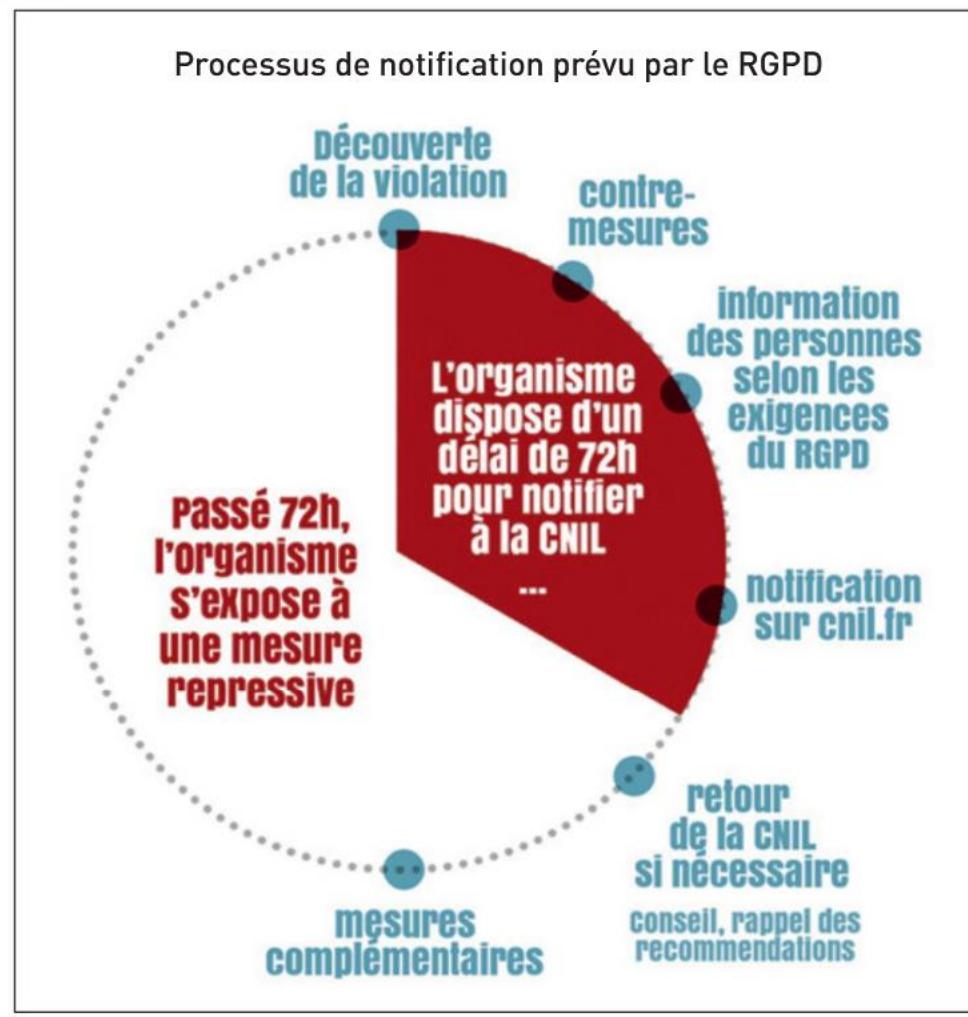
Les routeurs (ou passerelles) sont des équipements réseaux permettant de relier différents réseaux qui n'appartiennent pas au même réseau logique afin qu'ils puissent échanger des données. Pour acheminer les données vers les bons réseaux, le routeur dispose d'une table de routage qui lui indique la route à suivre. Dans un réseau local, le routeur, par l'intermédiaire de règles de sécurité, achemine ou non les informations vers différents réseaux internes. Cela permet ainsi d'instaurer une sécurité supplémentaire, qui ne permet pas le relais des trames de diffusion. Par exemple, avec un routeur Cisco, l'administrateur peut configurer des ACL (Access Control Lists) qui constituent des règles de filtrage sur chaque interface. On distingue les ACL standards, qui servent à filtrer les paquets uniquement sur les IP sources, et les ACL étendues, qui permettent de filtrer sur quasiment tous les champs des en-têtes IP, TCP et UDP.

Exemple : deny 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

Le réseau 192.168.1.0 /24 ne pourra pas communiquer avec le réseau 192.168.3.0 /24. Les paquets seront alors détruits au niveau du routeur.

Les obligations légales de notification en cas de failles de sécurité

Les failles de sécurité dans un SI peuvent entraîner la suppression, la modification ou encore la divulgation de données. Il est essentiel de connaître les obligations légales en cas d'incidents.



Le règlement général sur la protection des données (RGPD) impose aux responsables d'une organisation de documenter en interne les violations des données personnelles. Ils doivent aussi notifier les violations présentant un risque pour les droits et les libertés des personnes à la CNIL et, dans certains cas, lorsque le risque est élevé, aux personnes concernées.

I L'obligation d'assurer la sécurité du traitement

L'article 32 du RGPD prévoit pour le responsable du traitement ou le sous-traitant une obligation de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

II Les obligations de notification et de communication

1. Les délais

Le RGPD prévoit l'obligation de notification (articles 33 et 34) : les responsables de traitement sont tenus de notifier toute violation de données personnelles à l'autorité de contrôle compétente, et ce, dans un délai de 72 heures à compter de sa découverte.

➤ Voir lexique BTS SIO, p.221

…>

2. La communication

Les responsables de traitement doivent informer la personne concernée dans les meilleurs délais en cas de violation présentant un risque élevé pour les droits et les libertés. Plusieurs autorités de contrôle (la CNIL, l'ICO) ont établi des formulaires types pour les violations de données. La CNIL a également mis en place un téléservice de notification de violations. Le document récapitulatif de la notification à la CNIL permet de répondre à l'obligation de documentation interne.

Le téléservice mis en place par la CNIL permet de réaliser la notification. Il doit être utilisé uniquement par les responsables de traitement d'une organisation.



Les notifications de la CNIL
www.lienmini.fr/6988-502

III

La mise en place d'une politique interne pour les failles de sécurité

Les responsables de traitement doivent être en mesure de justifier leur politique en matière de sécurité, qui doit prévoir :

- l'organisation interne de l'entreprise ;
- les modalités de communication vis-à-vis des utilisateurs ;
- les relations contractuelles avec des acteurs extérieurs.

La preuve du respect des obligations liées à la sécurité des traitements implique la mise en place d'un cahier des incidents (distinct du registre des traitements), qui doit contenir :

- l'ensemble de la documentation relative à ces incidents ;
- la nature de la violation des données ;
- les catégories et le nombre approximatif des personnes concernées par la violation et les enregistrements des données des personnes concernées ;
- les conséquences probables de la violation des données ;
- les mesures prises ou envisagées pour atténuer les éventuelles conséquences négatives ou pour éviter que l'incident se reproduise.

IV

Les sanctions

En cas de non-respect des obligations précitées, les autorités de contrôle (en France, la CNIL) peuvent sanctionner tout responsable de traitement par des amendes administratives, pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial (article 83-4a du RGPD).

Par ailleurs, en droit français, le législateur a sanctionné pénalement tout accès ou maintien frauduleux dans un « système automatisé de traitement de données » (STAD), dont la définition est interprétée largement, de deux ans d'emprisonnement et 60 000 € d'amende (article 323-1 du Code pénal). Cette peine est portée à trois ans d'emprisonnement et 100 000 € d'amende lorsqu'il s'ensuit une modification ou une suppression de données, ou encore une altération du fonctionnement de ce système ou pour éviter que l'incident se reproduise.

1 QCM



Retrouvez ce QCM
en version interactive
www.lienmini.fr/6988-503

- 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, elle doit obligatoirement documenter les violations en interne.

- Vrai
- Faux

- 3** Le RGPD impose pour toute organisation une l'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 la 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 engendrés.

- 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 priviléges 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 priviléges



› Fiche savoirs technologiques 5 et 6

Situation

M. Rens est le président d'une association de réinsertion qui permet à des personnes à la recherche d'un emploi de bénéficier d'une aide technique dans l'élaboration des documents servant à postuler à une offre : CV, lettre de motivation, portefeuille de compétences, bilan de compétences, etc. Les personnes ont accès à un petit parc informatique pour réaliser des tâches bureautiques liées à leur recherche d'emploi. M. Rens souhaite mettre en œuvre une politique de sécurité des données des utilisateurs du parc informatique de l'association. Vous l'assitez dans cette mission.



- 1** Indiquez à M. Rens les bonnes pratiques à adopter en termes d'authentification et d'accréditation (annexes 1 et 2).
 - 2** M. Rens est l'administrateur des machines. Expliquez-lui quelles précautions il doit prendre concernant le compte administrateur.
 - 3** Indiquez quels priviléges il doit accorder à chaque utilisateur (annexe 3).
- M. Rens sait que le stockage des données à caractère personnel exige le respect d'obligations spécifiques.
- 4** Indiquez ces obligations en précisant pour chacune en quoi elle consiste (annexe 4).

Annexe 1 Analyser la présentation de la salle de formation

La salle de formation dispose de dix postes informatiques, contenant chacun des outils de traitement de texte, et d'un navigateur Internet. Pour utiliser un poste de travail, l'utilisateur doit se connecter à l'aide des éléments de connexion fournis par le formateur. Dans la salle de formation, le poste formateur dispose d'un dossier partagé dans lequel les différents participants peuvent stocker leurs données mais aussi accéder aux fichiers déposés par le formateur.

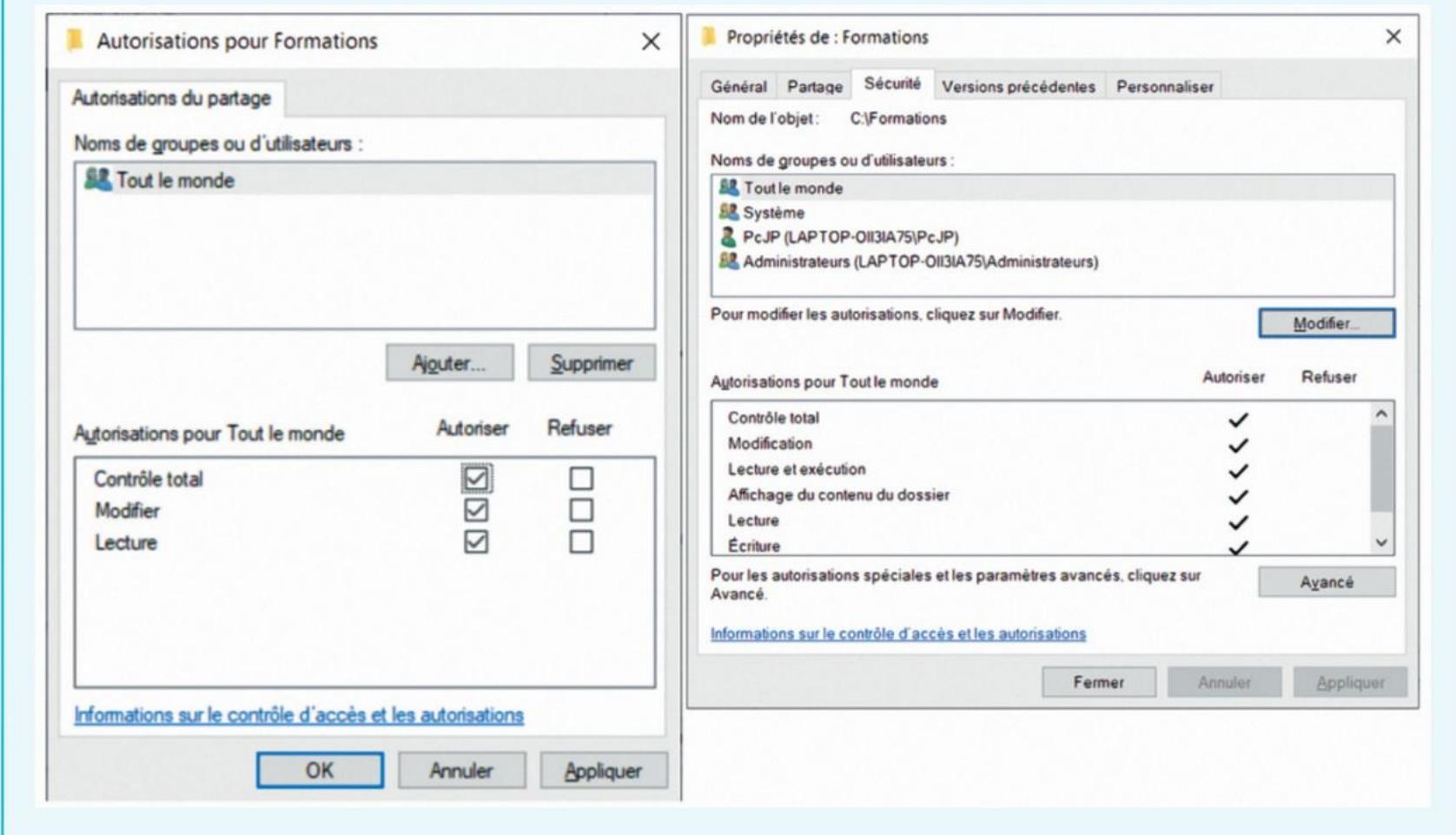
Annexe 2 Reconnaître les types de comptes

Chaque compte est créé selon le même modèle : participant-x, où x représente le numéro du poste sur lequel le participant ouvre une session.

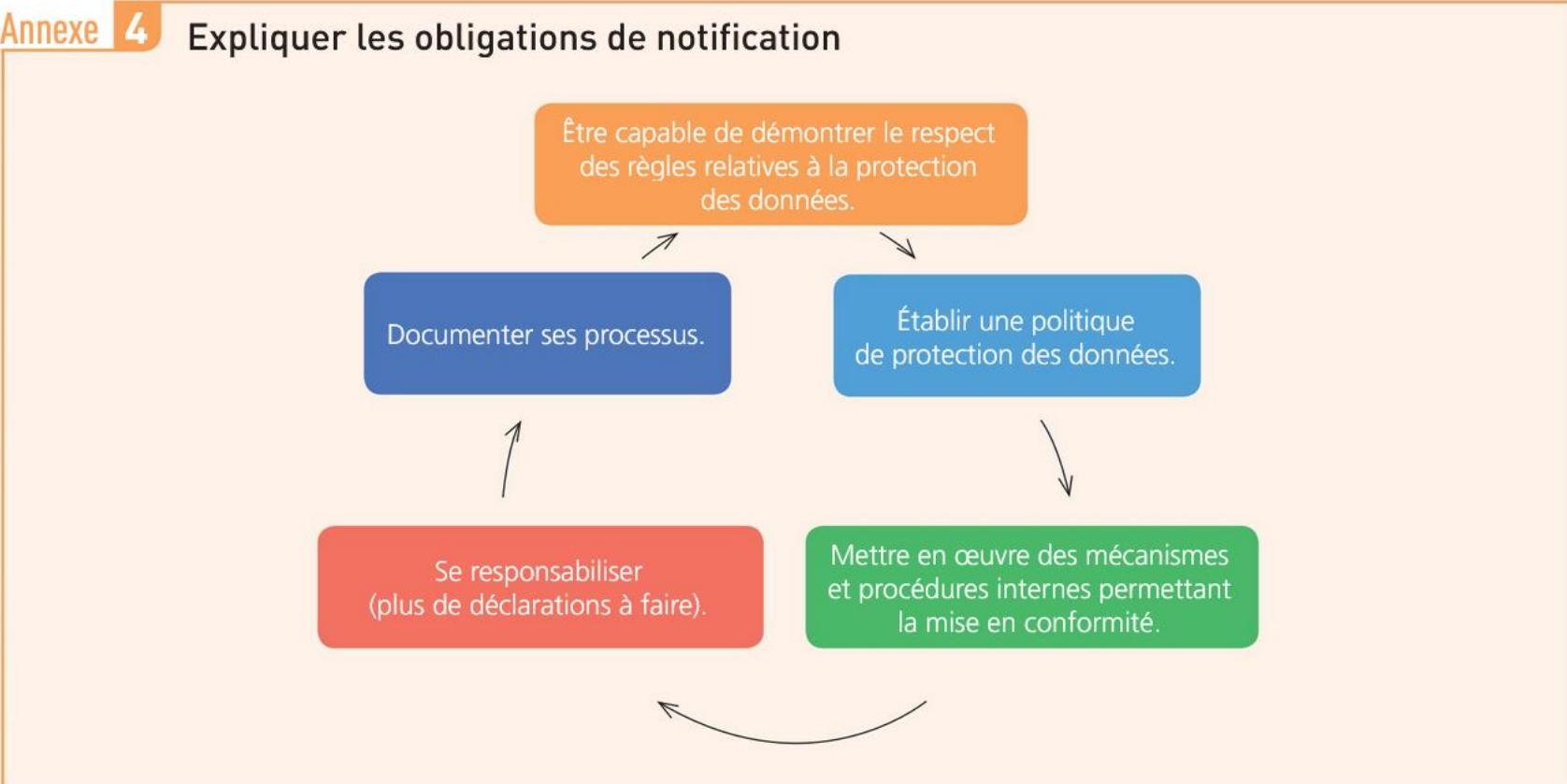
Propriétés de : Participant-1	
? X	
Général	Membre de Profil
<u>Membre de :</u>	
<input checked="" type="checkbox"/> Administrateurs <input checked="" type="checkbox"/> Utilisateurs	

Jusqu'à présent, le mot de passe et l'identifiant utilisés par M. Rens étaient identiques.

Annexe 3 Identifier les partages des données



Annexe 4 Expliquer les obligations de notification



3 Sécuriser les communications



› Fiche savoirs technologiques 7

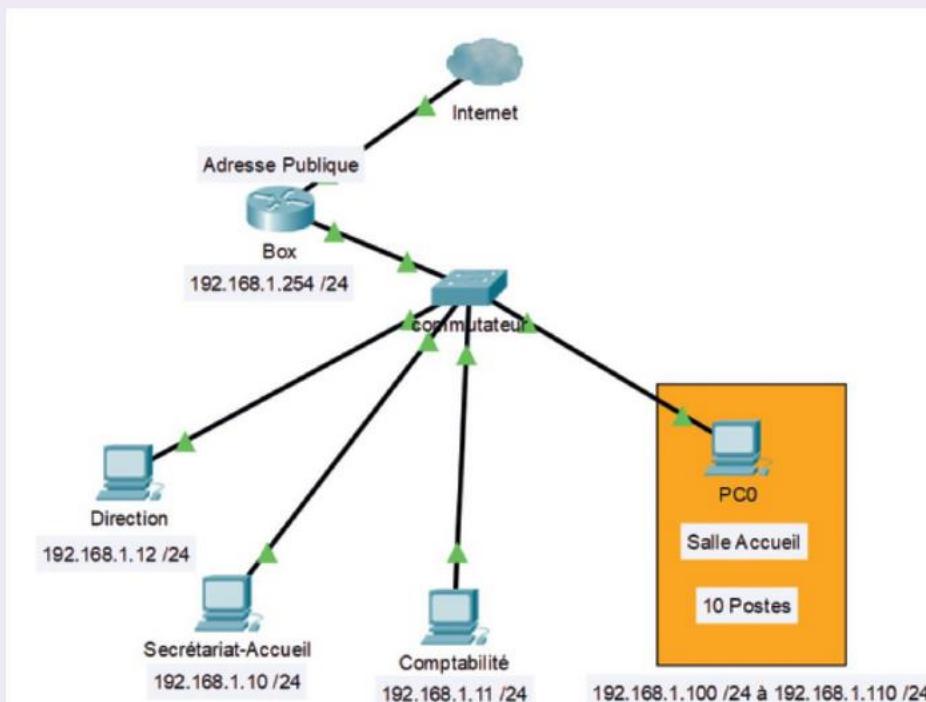
Situation

M. Rens reçoit les utilisateurs des ressources numériques dans une salle aménagée spécialement pour les activités de bureautique. Pour l'instant, cette salle est reliée au même réseau que les différents services de l'association (annexe). Actuellement, l'association ne dispose pas de budget pour acheter du matériel supplémentaire. Vous devez aider M. Rens à séparer le réseau (sans ajouter de matériel supplémentaire) pour apporter davantage de sécurité.

- 1** Indiquez à M. Rens de quelle solution il dispose pour segmenter le réseau.
 - 2** Rédigez une procédure pour répertorier les différentes étapes de réalisation de cette segmentation.
 - 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.
- › Fiche méthode 6, p. 215
- 4** Expliquez les conséquences de la segmentation logique du commutateur sur le routeur box (interface physique côté LAN).

Annexe

Infrastructure logique et physique



Évaluation 3

L'organisation cliente

Créé en 1978, le Greta (groupement d'établissements) des montagnes du Jura organise chaque année de nombreuses sessions de formation notamment sur l'appropriation des outils numériques (outils bureautique et Internet). Le Greta est situé dans les locaux du lycée de la Communication de Lons-le-Saunier.

Le réseau informatique est géré par la DSI du lycée mais celle-ci fait régulièrement appel à des prestataires extérieurs pour les tâches d'administration des services. La maintenance et la configuration du parc informatique restent à la charge de la DSI. Un formateur, qui intervient sur les sessions de formation aux outils numériques, a alerté la DSI en indiquant plusieurs dysfonctionnements au niveau du parc informatique de la salle de cours, qui pourraient remettre en cause l'intégrité du réseau local et donc des données.

Afin d'identifier plus spécifiquement ces différentes failles et proposer des solutions adaptées, la DSI a choisi de faire appel à la société Pent'39 dont l'activité principale est de réaliser des audits de sécurité des systèmes d'information.

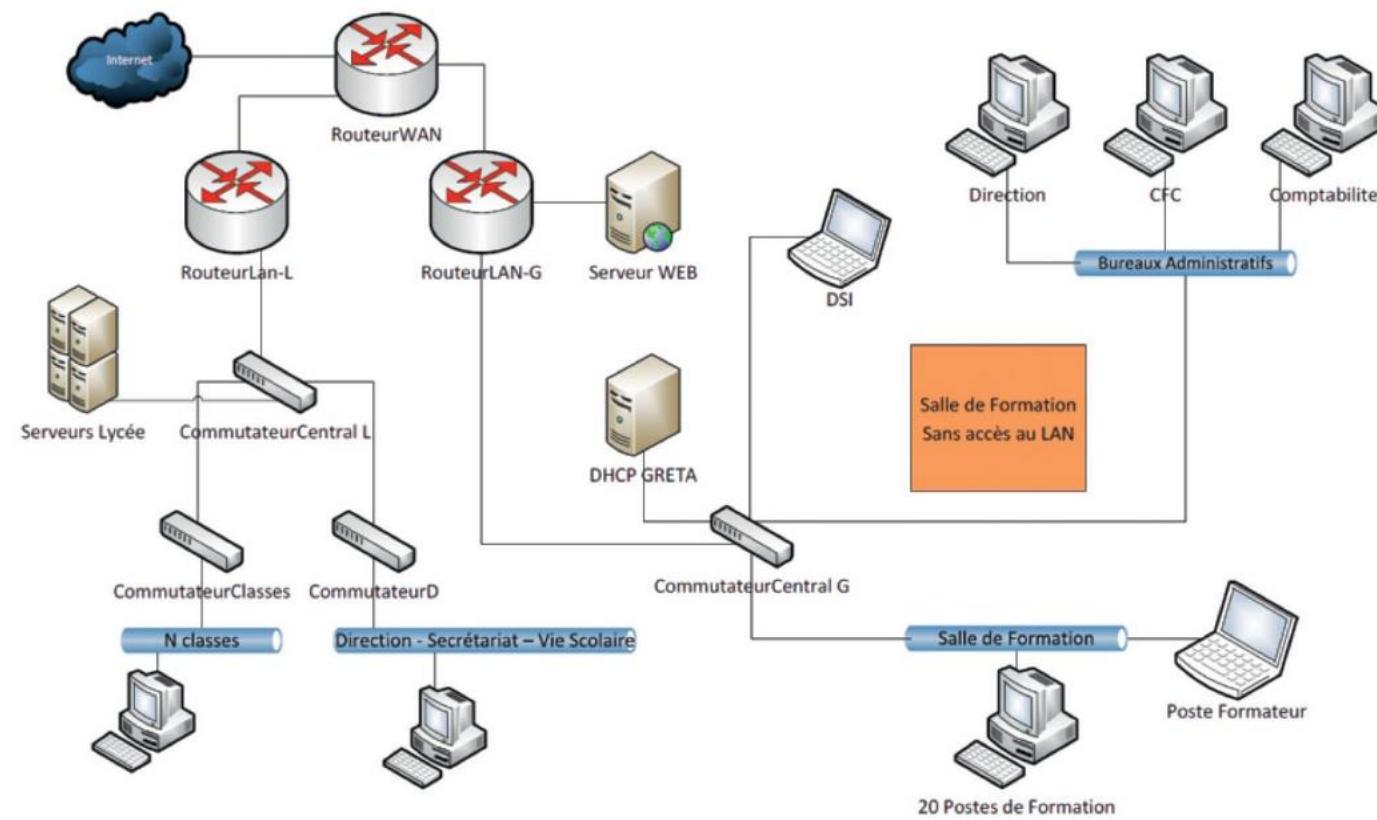


Le prestataire informatique

La société Pent'39, située à Orgelet, est spécialisée dans la réalisation d'audits de sécurité des systèmes d'information afin d'assurer un fonctionnement optimum des infrastructures réseaux de ses clients et d'apporter un accompagnement dans le support aux utilisateurs.

Vous intégrez cette société afin de prendre en charge l'audit de sécurité sur les différents processus de gestion du parc informatique du Greta.

Architecture réseau du GRETA



Votre mission

Votre mission consiste, dans un premier temps, à recenser les différentes failles de sécurité inhérentes à la gestion des postes de travail de la salle de formation. Dans un second temps, vous proposez des solutions adaptées pour assurer la sécurité des différentes sessions utilisateurs ainsi que leurs données. Pour réaliser ce travail, vous vous appuyez sur le dossier documentaire mis à votre disposition.

Missions

1 Identifier les failles de sécurité liées à la gestion du parc informatique de la salle de formation

Vous analysez la configuration des différents postes de travail afin de diagnostiquer les failles de sécurité. Pour cela, vous disposez d'un certain nombre d'informations concernant la configuration des postes mais également le processus de gestion des comptes utilisateurs.

- 1.1. Repérez les failles de sécurité liées à la configuration système des postes de travail et au processus d'authentification des utilisateurs.
- 1.2. Précisez en quoi la procédure d'attribution des autorisations et priviléges sur les dossiers de stockage des données ne permet pas de garantir la sécurité des données de chaque utilisateur.

2 Mettre en œuvre des configurations et outils pour garantir la sécurité du SI du Greta

Cette deuxième mission doit vous permettre d'émettre des propositions à la DSI du Greta pour améliorer la sécurité des sessions utilisateurs. Ces propositions peuvent inclure l'installation de nouveaux outils ou la modification de l'infrastructure logique et physique.

- 2.1. Indiquez quelles premières modifications vous pouvez apporter pour corriger les failles de sécurité identifiées précédemment.
- 2.2. Détaillez une segmentation possible pour sécuriser davantage les échanges dans le réseau local du Greta.
- 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.

Dossier documentaire

Document 1

Configuration des postes de travail

Observations réalisées sur les postes de travail de la salle de formation.



Protection contre les virus et menaces
Aucune action requise.



Protection du compte
Aucune action requise.



Pare-feu et protection du réseau
Les pare-feux sont désactivés.
Votre appareil est peut-être vulnérable.



Contrôle des applications et du navigateur
La fonctionnalité Vérifier les applications et les fichiers est désactivée, ce qui rend votre appareil vulnérable.

Document 2

Enquête auprès des utilisateurs

Le formateur a profité de sa dernière session de formation pour réaliser une enquête auprès des utilisateurs pour connaître leurs choix en termes de mots de passe. Le graphique ci-dessous en indique le résultat.



Document 3

Création des comptes et partages

Avant une formation, le formateur dispose de la liste des participants. Il crée un compte portant le nom de chacun et ajoute dans le dossier PartagesParticipant un sous-dossier de stockage des données pour chaque stagiaire. Ces actions sont réalisées sur le poste formateur.

Autorisations pour PartagesParticipant

Autorisations du partage

Noms de groupes ou d'utilisateurs :

- Tout le monde

Autorisations pour Tout le monde

	Autoriser	Refuser
Contrôle total	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modifier	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lecture	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Sécurité

Nom de l'objet : D:\PartagesParticipant

Noms de groupes ou d'utilisateurs :

- Utilisateurs authentifiés
- Système
- Administrateurs (LAPTOP-OII3IA75)\Administrateurs
- Utilisateurs (LAPTOP-OII3IA75)\Utilisateurs

Autorisations pour Utilisateurs authentifiés

	Autoriser	Refuser
Contrôle total	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modification	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lecture et exécution	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Affichage du contenu du dossier	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lecture	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Document 4

Stratégie de sécurité

Stratégie de sécurité locale

Fichier Action Affichage ?

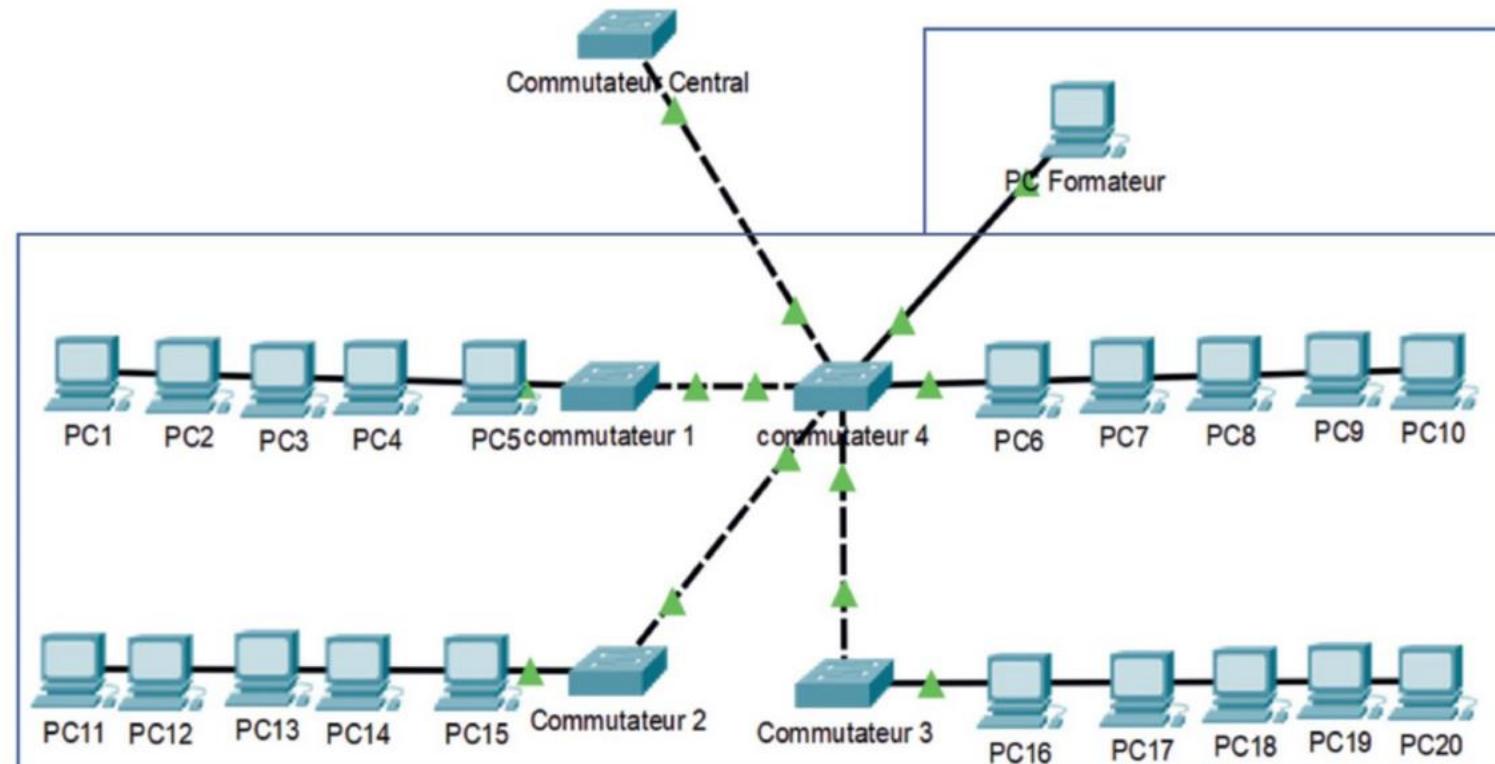
Paramètres de sécurité

- Stratégies de comptes
 - Stratégie de mot de passe
 - Stratégie de verrouillage du compte

Stratégie	Paramètre de sécurité
Conserver l'historique des mots de passe	0 mots de passe mémorisés
Durée de vie maximale du mot de passe	100 jours
Durée de vie minimale du mot de passe	0 jours
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Désactivé
Longueur minimale du mot de passe	0 caractère(s)

Document 5

Schéma logique et physique de la salle de formation



Le périmètre physique de la salle de formation est représenté par le cadre bleu. Les postes de travail sont configurés dans le Pool 192.168.50.0 /24 de nom PoolFormation du serveur DHCP. Les différents postes sont reliés aux commutateurs dans le VLAN 1. Ceux-ci disposent chacun d'un VLAN

de management (VLAN 99) en 192.168.99.0 /24 sur le port 24. Les commutateurs 1, 2 et 3 sont reliés au commutateur 4 à partir de leur port fa0/23 en mode TRUNK. Le commutateur 4 est relié au commutateur central également par son port fa0/23 en mode TRUNK.

Contexte 4

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



L'organisation cliente

Ecotri est une startup spécialisée dans la valorisation des déchets. Son fondateur, M. Legendre, souhaite créer une application qui indiquera à ses utilisateurs la poubelle à utiliser lorsqu'ils scanneront les codes-barres de leurs déchets à l'aide de leur smartphone. Plus un client scannera

de produits, plus il cumulera des offres promotionnelles adaptées à ses besoins. Ecotri s'est tournée vers la pépinière Cibeco pour bénéficier de ses locaux, équipés de serveurs, et de ses services, afin de développer cette application Web.

Le prestataire informatique

Cibeco est une pépinière spécialisée dans l'accompagnement de startups travaillant dans le domaine de la transition énergétique. Son objectif est de faciliter la création et le développement de ces jeunes entreprises en leur fournissant

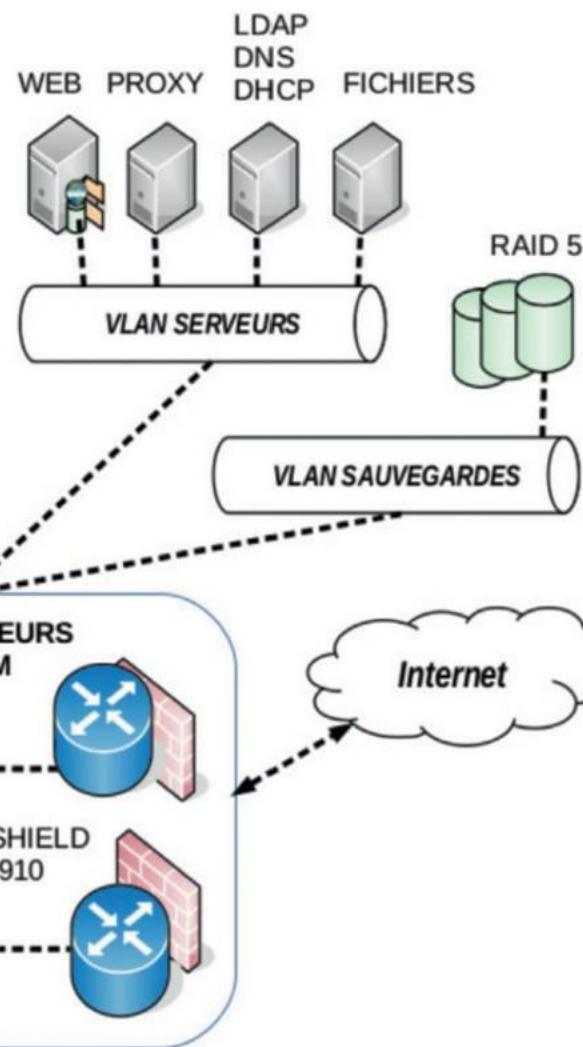
des locaux et des prestations informatiques. Elle est située à Provins, en Seine-et-Marne. Cibeco dispose de deux bâtiments de trois étages comportant chacun 10 salles. L'entreprise est gérée par ses deux fondatrices, Yaël et Sarah Darmon.

Contexte 4

Description du SI de l'organisation

Schéma général du réseau de Cibeco

- Utilisation de deux FAI
- Chaque client a son VLAN. VLAN de sauvegarde
- Archivage sur grappe RAID 5
- Pare-feu UTM de gestion unifiée des menaces
- Liens redondants entre commutateurs (STP)
- Agrégation de liaisons via la solution EtherChanne de Cisco
- Passerelle redondante sous forme de cluster VRRP
- Haute disponibilité des serveurs Web via la solution Haproxy
- Onduleurs, grappe de trois serveurs Web
- VirtualHost https via la solution Extended SSL de GlobalSign



Cahier des charges

Périmètre d'intervention

Les données du client Ecotri doivent être séparées de celles des autres clients. Cibeco se charge d'intervenir en cas de panne sur un serveur loué par Ecotri.

Exigence en termes de protection des données

L'application Web d'Ecotri devra faire l'objet de toutes les attentions en matière de sécurité pour minimiser les risques. Le contrat d'infogérance prévoit une

garantie de haute disponibilité sur l'application Web et les données manipulées. L'archivage des données doit se faire en conformité avec le RGPD. La confidentialité des flux manipulés au sein de l'infrastructure réseau doit être assurée.

Applications et équipements

Cibeco fournit au client Ecotri un serveur Web redondé pour sa future application Web.

Votre mission

Vous êtes accueilli(e) au sein de Cibeco en tant que nouveau(e) technicien(ne) chargé(e) d'accompagner le déploiement sécurisé de la solution du client Ecotri.

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

COMPÉTENCES

- Caractériser les risques liés à l'utilisation malveillante d'un service informatique
- Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité
- Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation

SAVOIRS ASSOCIÉS

- Protection et archivage des données : principes et techniques
- Chiffrement, authentification et preuve : principes et techniques
- Sécurité des applications Web : risques, menaces et protocoles
- Réglementation en matière de lutte contre la fraude informatique : infractions, sanctions

Situation professionnelle

Cibeco a développé une première version de l'application Web du client Ecotri. L'application a été testée. Le concept a convaincu les premiers utilisateurs, et le lancement est prévu à l'occasion du prochain Salon de la transition énergétique, avec le soutien de l'équipe marketing de Cibeco. Ecotri commence à attirer des utilisateurs et se fait connaître progressivement. Depuis quelques mois, la pépinière Cibeco fournit les locaux et les serveurs à son client. Encouragé par ce premier succès, M. Legendre, fondateur d'Ecotri, a de nouveaux projets pour sa startup.

Malheureusement, à la veille du Salon de la transition énergétique, une alerte signale une utilisation malveillante des serveurs de Cibeco touchant le système d'**archivage**. Cibeco constate que le site Web d'Ecotri a subi une attaque.

On vous confie alors trois missions : la mise en place d'un audit visant à caractériser les **risques** associés au système d'archivage de Cibeco ; le recensement des conséquences de l'attaque subie par Ecotri ; la réalisation d'un état des lieux des obligations légales liées à l'archivage et à la protection des données.



➤ Voir présentation générale, p. 135

Missions professionnelles

1

Caractériser les risques liés à une utilisation malveillante d'un système informatique

Afin d'identifier les failles qui ont permis l'attaque d'Ecotri, la gérante de Cibeco, Sarah Darmon, souhaite réaliser un audit sur la procédure d'archivage des données de la pépinière de l'entreprise. Votre rôle consiste à répertorier les risques.



Travail à faire

Dans un premier temps, vous devez identifier les risques liés à la politique d'archivage de la pépinière.

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

> Fiches savoirs technologiques 1 (p. 23) et 8
> Documents 1 et 2

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.

> Fiche savoirs technologiques 8
> Documents 1 et 2

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

> Fiche savoirs technologiques 1, p. 23
> Fiche savoirs CEJMA 2, p. 45
> Documents 1 et 2

Dans un second temps, vous étudiez la procédure de classification des risques identifiés afin de faciliter l'enregistrement des **incidents** si des actes malveillants se produisaient. Parmi les risques identifiés, deux ont attiré l'attention de la gérante de Cibeco :

- risque 1 : une personne malveillante accède frauduleusement aux données archivées ;
- risque 2 : une personne malveillante modifie frauduleusement le contenu 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.

> Fiche savoirs technologiques 1, p. 23
> Document 3

> Voir lexique BTS SIO, p. 221

Dossier documentaire

Document 1 Entretien avec la responsable de Cibeco sur la politique d'archivage des données de la pépinière

Vous : Quelles sont les données archivées au sein de Cibeco ?

S. Darmon : Tout ce que la loi nous impose d'archiver, c'est-à-dire les transactions avec les clients de la pépinière, les données comptables et financières, ainsi que les données liées au trafic réseau de nos clients. Cela inclut les transactions bancaires réalisées avec nos clients.

Vous : Comment organisez-vous cet archivage ?

S. Darmon : Nous disposons d'un serveur dédié aux opérations d'archivage, avec un disque d'une capacité de 500 Go. Je m'occupe personnellement d'alimenter ce serveur. Pour cela, je copie les données à archiver sur une clé USB, puis je les transfère sur le serveur

dédié. Je fais en sorte de réaliser cet archivage tous les jours à 18 h 00.

Vous : Comment ce serveur d'archivage est-il protégé ?

S. Darmon : Tous nos serveurs, ainsi que ceux de nos clients, sont installés dans une salle protégée par un digicode. L'accès au serveur d'archivage de Cibeco nécessite de déverrouiller un écran de veille avec un mot de passe. Je suis la seule à connaître le mot de passe et l'écran se met automatiquement en veille au bout de cinq minutes d'inactivité. Quant à nos clients, seuls ceux qui louent des serveurs peuvent accéder à cette salle et ont connaissance du digicode.

Document 2 La description de la solution technique d'archivage de Cibeco



Les données à archiver sont régulièrement copiées sur une clé USB.

Transfert régulier via un port USB librement accessible sur le serveur d'archivage



Serveur d'archivage sous Windows : un seul serveur pour toutes les archives
Capacité de stockage : 500 Go



Les données archivées ne sont pas chiffrées.



Accès aux archives par saisie d'un login et d'un mot de passe



Rotation des archives : les archives sont conservées pendant 2 ans puis le disque est formaté.

Document 3 Extrait du ticket de déclaration d'un incident

Ticket de déclaration d'un incident	
Date de l'incident : / /	Description :
Niveau de gravité :	
<input type="checkbox"/> Négligeable	
<input type="checkbox"/> Limité	
<input type="checkbox"/> Important	
<input type="checkbox"/> Maximal	

Missions professionnelles

Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité

L'application Web du client Ecotri vient de subir une attaque importante. Ecotri se tourne vers Cibeco, qui a développé cette application. Sarah Darmon vous demande de réaliser un état des lieux des conséquences de cette attaque.



Travail à faire

1. Recensez les conséquences techniques de l'attaque subie par Ecotri, en fonction des critères DIC (disponibilité, intégrité, confidentialité).
 - > Fiche savoirs technologiques 2, p. 25
 - > Fiche savoirs CEJMA 1, p. 28
 - > Documents 1 et 2
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.
 - > Document 3
 - > Fiche savoirs technologiques 10
3. Relevez les conséquences humaines et financières de cette attaque pour Ecotri.
 - > Documents 1 à 4
 - > Fiche savoirs CEJMA 4, p. 71
4. Identifiez les conséquences juridiques possibles pour l'auteur de l'attaque.
L'adresse IP de l'attaquant peut-elle être identifiée ?
 - > Fiche savoirs technologiques 8
 - > Fiche savoirs CEJMA 8
 - > Document 5

Dossier documentaire

Document 1 Extrait de votre conversation téléphonique avec le responsable d'Ecotri au sujet de l'attaque

Vous : Que se passe-t-il exactement ?

Ecotri : C'est une catastrophe, la page d'accueil du forum sur le site a été modifiée et affiche la liste de tous les membres d'Ecotri, avec leurs coordonnées. Je n'arrête pas de recevoir des appels de clients mécontents, je ne sais plus quoi faire...

Vous : Comment vous êtes-vous rendu compte du problème ?

Ecotri : Par les appels répétés de mes clients ! Non seulement, leurs coordonnées sont affichées publiquement

sur le forum, mais en plus le service de valorisation des déchets n'est plus fonctionnel. Je suis complètement paralysé. Inutile de vous dire ce que mes clients rapportent de cet incident sur les réseaux sociaux. C'est une catastrophe, je suis tout à fait démunis face à la situation. Que pouvez-vous faire en tant que développeur du site ? Aidez-moi, il y a urgence !

Vous : C'est noté. Je vais immédiatement faire un état des lieux de la situation.

➤ Voir lexique BTS SIO, p. 221

Document 2 Un extrait du forum du site Web d'Ecotri après l'attaque

Ecotri
Recyclez, récoltez !

Bienvenue sur le forum d'Ecotri dédié à la valorisation des déchets. Ici, vous pouvez échanger sur les bonnes pratiques de recyclage. Faites-nous part de votre expérience. Tout message posté fera l'objet d'une modération.

HACKED BY
@ST_BENJ!!

Thèmes	Voici la liste de tous les membres
Compost	Jean Dupont, 6 rue du marché 65007 Grandouvrage, 01 55 51 01 01
Déchets carton	Antoine Rubaud, 2 place de l'église 91230 Villeneuve-le-Livre, 06 51 51 48 01
L'appli Ecotri	Andrey Rebanov, 25 rue du métro 25035 Charleville, 06 01 99 99 98
À vos poubelles	Patricle Elnawy, 6 impasse de la cour 55023 Mandre-les-Hauts, 04 25 99 88 96
	Hubert Garand, 56 bis rue de la volonté 45698 Montgravas, 03 03 05 04 01

Document 3 La procédure de développement Web des formulaires par Cibeco

Cibeco utilise la procédure suivante pour développer ses formulaires en PHP :

- Étape n° 1

Le code source vérifie que la saisie n'est pas vide.

- Étape n° 2

Les données saisies par l'utilisateur sont stockées en l'état dans des variables.

- Étape n° 3

Ces variables servent de paramètres à la requête SQL d'insertion.

Jean Dupont

Titre du message :

Saisir un titre

Contenu du message :

Saisir un message

Valider

Ecotri
Recyclez, récoltez !

Cibeco vous fournit un exemple de code produit pour le développement de ses formulaires :

```
1- <?php
2- $idMsg = $_SESSION['IDMSG']; $idAuteur = $_SESSION['AUTEUR'];
3- //On vérifie que les champs du formulaire sont remplis.
4- if ( isset( $_POST['titre'] ) && isset( $_POST['message'] ) ) {
5-     //Récupération des données saisies par l'utilisateur.
6-     $ParamTitre = $_POST['titre'];
7-     $ParamMessage = $_POST['message'];
8-     //Ajout dans la base de données des données saisies.
9-     $ajout = "INSERT INTO forum VALUES('$idMsg','$ParamTitre',
10-         '$ParamMessage','$idAuteur')";
11-     mysqli_query($ajout);
12- }
```

➤ Voir lexique BTS SIO, p. 221

Missions professionnelles

Document 4 Un extrait des commentaires concernant Ecotri sur les réseaux sociaux

Jean Dupont Mes coordonnées visibles en public sur le site d'Ecotri! Un tel manque de sécurité est inadmissible, je me renseigne pour déposer PLAINE ! 😥😥

J'aime · Répondre · Contacter - 1 sem

→ Voir les réponses précédentes

Audrey Rabanov En effet, le site a été hacké. J'ai appelé pour le signaler mais le gérant est en panique, je comprends qu'il soit stressé, mais je suis en colère ! 😥😅 Pour moi, c'est fini Ecotri, je résilie mon abonnement !

J'aime · Répondre - 1 sem

→ Voir plus de réponses

Hubert Garand Ecotri, comme son nom l'indique, c'est une application détritus. 😤😤 Donc abonnement à la poubelle !

J'aime · Répondre · Contacter - 1 sem

Antoine Rubaud J'ai aussi appelé pour le signaler, c'est le gérant qui a répondu et il est effondré. 😥😅 Je lui ai demandé de désactiver son site pour ne plus que mes coordonnées soient visibles mais il a l'air complètement perdu. Je veux bien compatir, mais il aurait du prévoir ce risque ! 😥

→ Voir plus de réponses

Document 5 Un extrait des journaux systèmes du serveur Web d'Ecotri

- L'extraction des journaux systèmes

Elle est effectuée avec un filtre sur la date du jour de l'attaque.

Les journaux donnent les informations suivantes sur les accès au site Web d'Ecotri :

adresse_ip	date_et_heure	url_des_pages	taille_chargée
82.89.34.7	Lundi 11 nov. 2019	eco-tri.fr/forum	73897
82.89.34.7	Lundi 11 nov. 2019	eco-tri.fr/forum/img.jpeg	8542
82.89.34.7	Lundi 11 nov. 2019	eco-tri.fr/forum/header.css	25000
82.89.34.7	Lundi 11 nov. 2019	eco-tri.fr/forum/new_msg	896542
82.89.34.7	Lundi 11 nov. 2019	eco-tri.fr/forum/valider	12540
82.89.34.7	Lundi 11 nov. 2019	eco-tri.fr/forum/valider.ok.jpeg	12589

- L'utilisation des journaux systèmes

La gérante de Cibeco a transmis cette extraction aux autorités judiciaires en accompagnement de sa plainte suite à l'attaque subie par le site Web de son client Ecotri.

➤ Voir lexique BTS SIO, p. 221

Missions professionnelles

3

Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation

Suite aux dernières attaques subies par la pépinière et son client Ecotri, la gérante de Cibeco s'inquiète des risques de poursuites judiciaires à son encontre. Elle vous demande de rédiger un rapport sur les obligations légales en matière d'archivage et de protection des données.

Travail à faire

- Identifiez, en argumentant, les obligations légales non respectées par Cibeco en matière de sécurisation physique des archives.
 - Documents 1 et 2
 - Fiche savoirs technologiques 8
- La procédure de traçabilité des accès aux archives de Cibeco est-t-elle conforme à la réglementation ?
 - Document 2
 - Fiche savoirs technologiques 8
- 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.
 - Fiches savoirs technologiques 8 et 9
 - Fiche savoirs CEJMA 1, p. 28
 - Document 3
- 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.
 - Document 3
 - Fiches savoirs technologiques 5 (p. 119), 9 et 10

Dossier documentaire

Document 1 L'état des lieux sur la sécurité physique des archives de Cibeco

Après un entretien avec la gérante de Cibeco sur la sécurité physique des archives, un bilan technique est dressé sous forme de tableau :

Éléments à protéger	Constatations
Détecteur de fumée	Seulement dans les salles communes de la pépinière (hall d'accueil et bureaux).
Climatisation	Dans toutes les salles.
Extincteurs	Uniquement des extincteurs manuels dans les salles communes.
Perte de données archivées	Des copies des archives sont effectuées manuellement tous les six mois et conservées sur clé USB.
Accès aux archives	Les archives sont stockées sur un serveur situé dans la même salle que celle des serveurs des clients.
Contrôle d'accès	Alarme en cas d'intrusion la nuit et présence d'un digicode sur la porte d'entrée de la salle des serveurs.
Vidéoprotection	Non installée pour le moment.
Serveur d'archivage	Serveur au format tour, absence de câble antivol.

➤ Voir lexique BTS SIO, p. 221

Missions professionnelles

Document 2 La traçabilité des accès aux archives de Cibeco

Chaque accès aux archives est noté sur un formulaire papier où il faut indiquer la date, l'heure et le motif de la consultation des archives. Lors de l'état des lieux sur la procédure d'archivage, la gérante de Cibeco vous indique que le dernier accès date du 24 octobre 202N à 17 h 00. Elle vous fournit le formulaire à la date du jour. Son contenu complet est le suivant :

Cibeco – historique des accès aux archives		
Date	Heure	Motif
03/01/202N	15 h 35	Demande accès client Dupont - OK
02/02/202N	14 h 35	Transfert des archives compra 2018
05/03/202N	15 h 00	Suppression archives 2017 - OK

Document 3 Les informations concernant l'administration du serveur miRDB

• La page d'administration du serveur de base de données miRDB de Cibeco

Elle permet d'accéder aux informations stockées sur le serveur de base de données miRDB. Ce serveur contient toutes les données d'administration sur les transactions de Cibeco avec ses clients.



• L'accès à la page Web d'administration du serveur miRDB de Cibeco

Un seul compte est utilisé. Ce compte est partagé par Yaël et Sarah Darmon, gérantes de Cibeco, ainsi que tous les collaborateurs techniques ayant besoin légitimement de consulter les données des transactions.

• Les journaux systèmes du serveur miRDB de Cibeco

Les journaux systèmes, permettant de tracer les accès au serveur de base de données miRDB de Cibeco, sont désactivés en raison du faible espace disque disponible.

Protéger une application Web en appliquant un codage sécurisé



› Fiche savoirs technologiques 10

Cibeco vous propose de suivre une formation sur le thème de la sécurisation des applications Web. Une architecture réseau a été spécialement conçue pour cette formation. Durant cette session, vous jouez successivement deux rôles :

- le hacker : vous allez attaquer un site Web interne destiné à la formation afin de faire apparaître la liste de tous les membres du site ;
- le développeur : vous devez protéger ce site Web via l'application de contre-mesures de codage sécurisé.

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.
› 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.
› *DELAGRAVE-LAB-THEM4.ova* : www.lienmini.fr/6988-601
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.
› Document 1
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.
› Document 1

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

Dans le scénario testé, la page Web cible est *user-info.php*. Le niveau de sécurité doit rester à 0 sur Mutillidae.

5. Réalisez l'injection SQL en suivant les instructions figurant dans le fichier *LAB-THEME4-CHAP6-DEFI.txt* présent sur le bureau de la machine *DELAGRAVE-CLIENT-HACKER-UBUNTU*. Que constatez-vous ?
› Documents 2 et 3

ÉTAPE 3 La contre-mesure de codage sécurisé

La page Web cible est toujours *user-info.php*. Il s'agit de configurer un codage sécurisé.

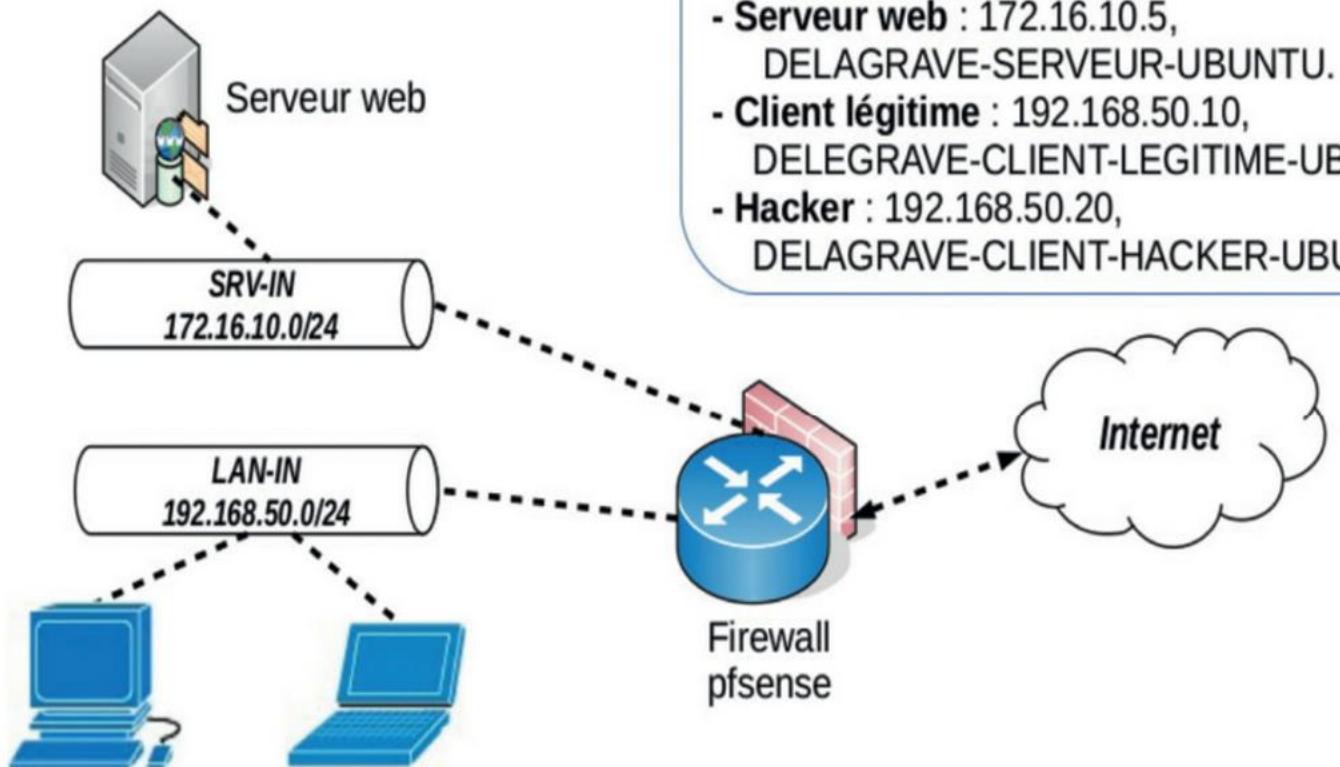
6. Positionnez le niveau de sécurité à 5 sur Mutillidae, puis reproduisez les étapes permettant de réaliser l'injection SQL. Que constatez-vous ?
› Documents 3 et 4
7. Comparez le code source de la page *user-info.php* dans sa version sécurisée et dans sa version non sécurisée. Quelle partie du code permet d'éviter l'injection SQL ? Que pouvez-vous en déduire en matière de bonnes pratiques de codage sécurisé ?
› Documents 3 et 4
› Fiche savoirs technologiques 10

Document 1 L'environnement de travail

Tout le travail de formation s'effectue au sein d'un réseau composé de quatre machines virtuelles. Aucun site Web extérieur ne fait l'objet d'une attaque. L'accès à Internet sert uniquement au téléchargement de VirtualBox et des machines virtuelles.

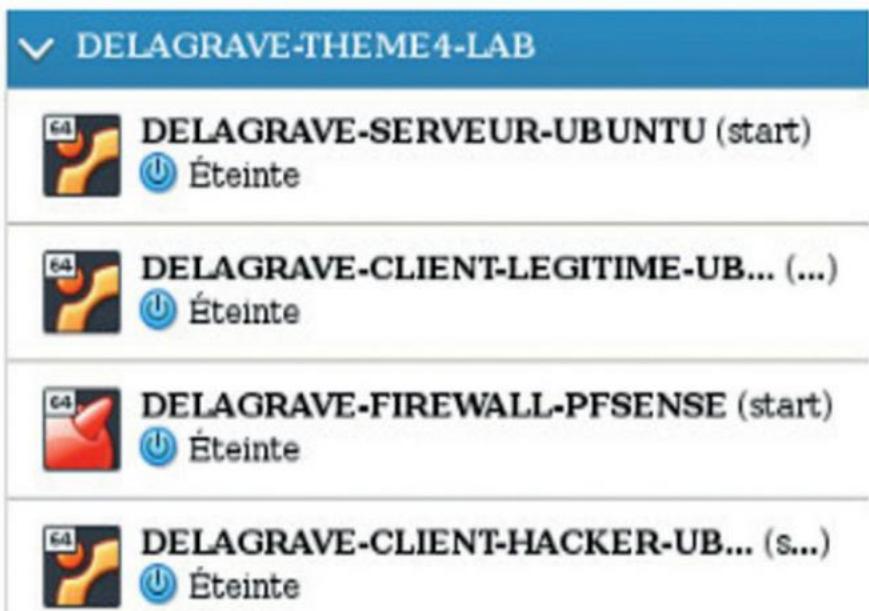
- Le réseau informatique dédié à la formation

Schéma du réseau informatique utilisé dans le cadre de la formation sur la sécurité des applications web



- Réseau **LAN-IN** : 192.168.50.0/24,
Passerelle : 192.168.50.254.
- Réseau **SRV-IN** : 172.16.10.0/24,
Passerelle : 172.16.10.254.
- Serveur web : 172.16.10.5,
DELAGRAVE-SERVEUR-UBUNTU.
- Client légitime : 192.168.50.10,
DELAGRAVE-CLIENT-LEGITIME-UBUNTU.
- Hacker : 192.168.50.20,
DELAGRAVE-CLIENT-HACKER-UBUNTU.

- L'importation des machines virtuelles avec le logiciel VirtualBox



•••

• Les descriptions des machines utilisées

Machines	Descriptions	Identifiants
DELAGRAVE-SERVEUR-UBUNTU	Cette machine est un serveur Web contenant le site Web à attaquer. Elle se nomme Mutillidae.	Login : prof Mot de passe : prof
DELAGRAVE-CLIENT-LEGITIME-UBUNTU	Il s'agit de la machine d'un utilisateur légitime du réseau.	Login : prof Mot de passe : prof
DELAGRAVE-CLIENT-HACKER-UBUNTU	C'est la machine du hacker. Elle contient les logiciels nécessaires aux manipulations demandées.	Login : prof Mot de passe : prof
DELAGRAVE-FIREWALL-PFSENSE	Il s'agit du routeur du contexte abordé.	Login : admin Mot de passe : pfsense

Document 2 Le scénario de l'attaque

Présentation du scénario

Un utilisateur malveillant réalise une injection SQL afin d'afficher la liste de tous les membres du site Web Mutillidae.

Cet affichage constitue une brèche de confidentialité car seul l'administrateur du site Web est censé voir ces informations.



Le site Web cible Mutillidae

Mutillidae est une application Web pédagogique intentionnellement vulnérable développée par le groupe OWASP. Cette application permet de tester les attaques et d'apprendre à coder de manière sécurisée.

Le code source de chaque page contient une version sécurisée et une version non sécurisée.

L'injection SQL

Il s'agit d'une faille de sécurité qui permet d'injecter dans la requête SQL en cours d'exécution un morceau de requête non prévu par le système.

Dans le scénario d'attaque testé, l'objectif est de valider une requête permettant d'afficher la liste de tous les membres du site.

Document 3 Les niveaux de sécurité du site Web cible Mutillidae

Le code source de chaque page Web sur Mutillidae peut être observé et analysé.

Les pages PHP de l'application sont présentes dans le répertoire suivant sur le serveur Web : `/var/www/html/mutillidae`.

Chaque page comprend les trois niveaux de sécurité indiqués ci-dessous :

Niveaux	Significations
Niveau 0	Aucune sécurité
Niveau 1	Sécurité partielle
Niveau 5	Sécurité complète

Le niveau de sécurité par défaut de chaque page est de 0. Ce niveau peut être modifié en cliquant sur le bouton *Toggle Security* situé en haut de l'application Mutillidae :

Toggle Security



Security Level: 0 (Hosed)

Document 4 La contre-mesure de codage sécurisé

La contre-mesure consiste à appliquer le niveau de sécurité 5 sur Mutillidae et à étudier le code source correspondant.

L'activation d'un codage sécurisé permet d'éviter l'attaque de type injection SQL.

Dans le cas de l'injection SQL, deux types de vérifications sont effectués :

- la longueur des données saisies afin d'éviter l'injection de code malveillant ;
- la vérification du contenu saisi via une liste noire de caractères interdits généralement associés à du code malveillant.

Chaque page Web de l'application Mutillidae permet de se positionner en mode de codage sécurisé en utilisant la séquence suivante :

```
switch ($_SESSION[«security-level»]) {
    Case «0» : //Code non sécurisé.
    ...
    Case «5» : //Code sécurisé.
}
```

Le niveau de sécurité 5 renvoie vers du code source associé à des fonctions qui permettent des contrôles plus avancés pour éviter les principales attaques.

```
3   switch ($_SESSION["security-level"]){
4       case "0": // This code is insecure
5           $lEnableHTMLControls = FALSE;
6           $lFormMethod = "GET";
7           $lEnableJavaScriptValidation = FALSE;
8           $lProtectAgainstMethodTampering = FALSE;
9           $lEncodeOutput = FALSE;
10          break;
11
12      case "1": // This code is insecure
13          $lEnableHTMLControls = TRUE;
14          $lFormMethod = "GET";
15          $lEnableJavaScriptValidation = TRUE;
16          $lProtectAgainstMethodTampering = FALSE;
17          $lEncodeOutput = FALSE;
18          break;
```

La protection et l'archivage des données

I

Définition

Une archive est une somme de documents classée afin d'être conservée durablement. La procédure d'archivage peut être effectuée via des supports papiers ou numériques. Il ne faut pas confondre l'archivage et la sauvegarde.

Sauvegarde	Archivage
 <p>Duplication de données en cours de traitement par le système informatique, en vue de pouvoir les restaurer.</p>	 <p>Copie d'anciennes données qui ne sont plus en cours de traitement en vue de leur conservation.</p>

II

L'archivage des données à caractère personnel

La **CNIL** définit trois phases successives dans le cycle de conservation des données de l'organisation :

Base active	Base des données en cours d'utilisation. Pendant toute la durée des traitements des données, celles-ci doivent faire l'objet de sauvegardes régulières.
Archivage intermédiaire	Les données issues des transactions réalisées avec des cartes bancaires doivent être conservées pendant une durée de 13 mois en cas de contestation d'un client (article L. 133-24 du Code monétaire et financier).
Archivage définitif	L'intérêt public peut parfois justifier que certaines données ne fassent l'objet d'aucune destruction. Ces archives sont gérées par le service des archives territorialement compétent (conditions du livre II du Code du patrimoine).

III

Les techniques de protection des données de l'entreprise

Quel que soit le type d'archivage effectué, l'administrateur réseau doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données archivées contre la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé.

Ces mesures doivent assurer un niveau de sécurité correspondant aux risques présentés. Le non-respect de cette obligation de sécurité est sanctionné par l'article 226-17 du Code pénal qui prévoit une peine de cinq ans d'emprisonnement et 300 000 euros d'amende.



➤ Voir lexique BTS SIO, p. 221

...>

Les techniques indiquées ci-dessous peuvent être utilisées afin de protéger les données :

Éléments à protéger	Techniques de protection
Protection physique des locaux	Présence d'un digicode, climatisation, protection incendie, séparation de la salle d'archivage des autres salles.
Gestion des habilitations	Seules les personnes habilitées ont accès aux archives. Il convient donc de recenser ces personnes et de limiter leurs droits d'accès au périmètre de consultation autorisé.
Traçabilité	Toute consultation des archives doit faire l'objet d'un enregistrement automatisé (date, heure, nom de la personne doivent être notés). Il ne doit surtout pas exister de compte unique partagé pour accéder aux supports d'archivage sur des serveurs.
Types de supports numériques utilisés	La CNIL déconseille d'utiliser des CD et des DVD inscriptibles car leur durée de vie dépasse rarement les quatre ou cinq ans. Utiliser plutôt des disques durs ou des bandes magnétiques.
Accessibilité	Classement des archives ergonomique pour répondre rapidement à une demande d'accès.
Confidentialité	Chiffrement des archives requis si elles contiennent des informations confidentielles.
Taille des archives	Compression des archives pour limiter la place occupée sur les supports informatiques.
Risque de perte	Copie en double des archives. Conserver la copie dans un lieu différent.

IV

La durée de conservation des archivess

Au terme de la réalisation du traitement, les données doivent être effacées, archivées, ou faire l'objet d'un processus d'anonymisation. L'anonymisation consiste à rendre invisible le nom d'un utilisateur concerné par une connexion. Par exemple, lorsqu'un administrateur non habilité consulte les journaux système, il ne voit pas le nom de l'utilisateur à l'origine de la connexion.

Les données archivées ne doivent être conservées que le temps nécessaire à l'accomplissement de l'objectif poursuivi.

Les durées d'archivage dépendent des types de données concernées :

- données relatives à la gestion du personnel : cinq ans à compter de la date à laquelle le salarié a quitté l'entreprise (article L. 1221-26 du Code du travail) ;
- bulletins de paie : cinq ans (article L. 3243-4 du Code du travail) ;
- documents comptables : dix ans (article L. 123-22 du Code de commerce) ;
- documents fiscaux : six ans (article L. 102 B du Livre des procédures fiscales) ;
- données de trafic collectées pour des besoins de recherche, de constatation et de poursuite des infractions pénales : un an à compter du jour d'enregistrement.

Fiche savoirs technologiques 9

Le chiffrement, l'authentification et la preuve

I

Définitions

Le **chiffrement** est un procédé de cryptographie qui rend la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement. Le chiffrement permet d'assurer la confidentialité des informations échangées.

L'**authentification** permet à une personne d'accéder à une ressource informatique en prouvant son identité (par un mot de passe par exemple).

La **preuve** (Fiches savoirs technologiques 2, p. 25) permet de faire la démonstration de la réalité d'un fait auprès d'un autorité judiciaire. Elle peut être numérique (saisie et examen d'un disque dur, par exemple) et, pour être valable, doit respecter certaines procédures légales.

II

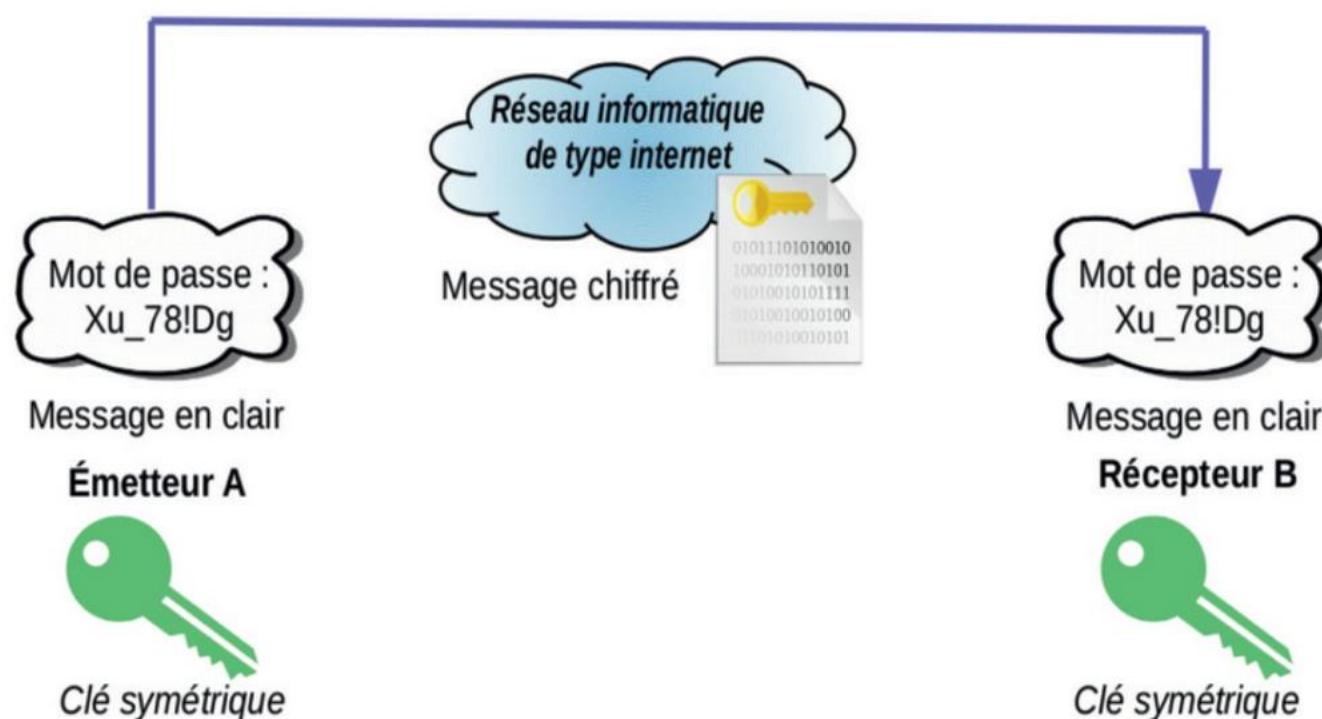
Les techniques

1. Les techniques de chiffrement

Le chiffrement permet de protéger la confidentialité des données d'une organisation. En effet, un flux non chiffré peut être intercepté par une personne malveillante, même si un mot de passe très solide est utilisé.

Deux types de chiffrements peuvent être utilisés :

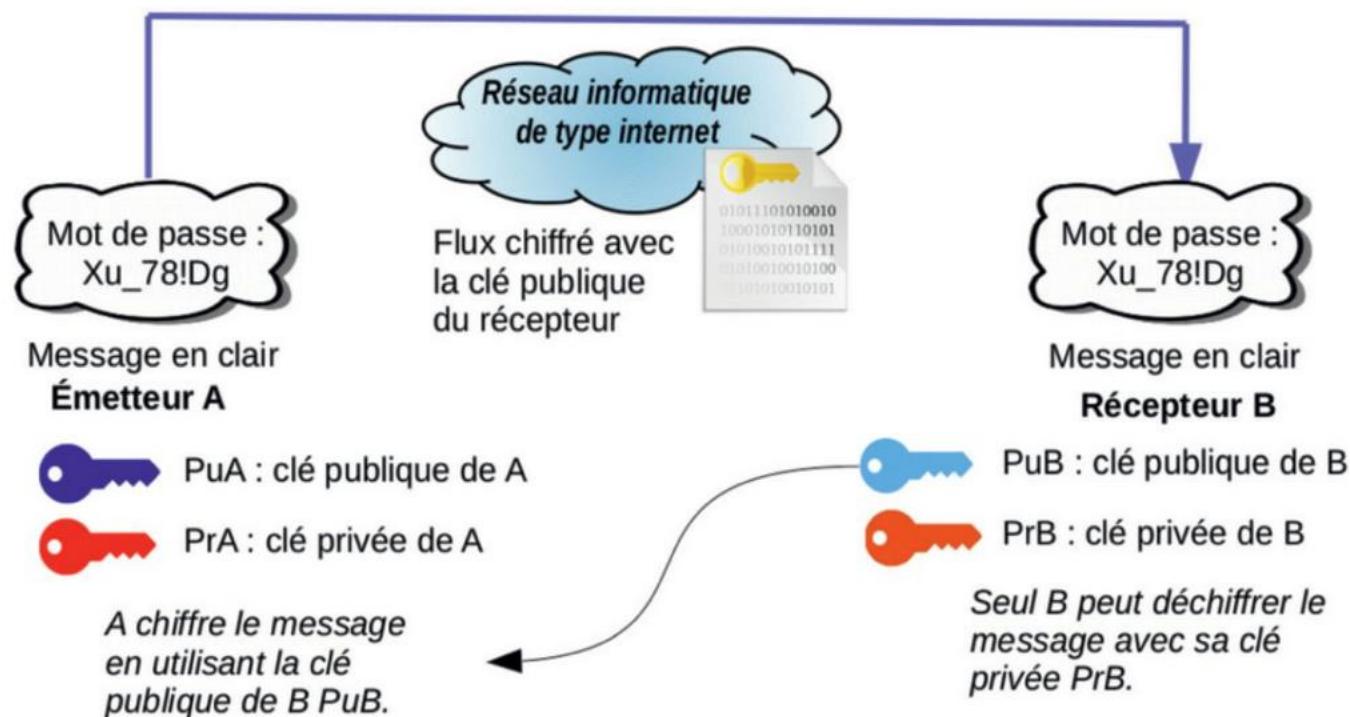
- le **chiffrement symétrique** : une clé unique est utilisée pour chiffrer et déchiffrer le message. Avec cette méthode, le chiffrement est simple. Sa faiblesse réside dans la transmission de la clé à un correspondant.



La clé peut être interceptée par un tiers, d'où la nécessité d'utiliser un chiffrement asymétrique en complément.



- le chiffrement asymétrique : deux clés (clé publique, clé privée) sont nécessaires pour chiffrer et déchiffrer le message. La clé publique peut être transmise à des tiers et la clé privée est confidentielle. Cette technique permet de transmettre la clé de chiffrement symétrique à un tiers de manière confidentielle.



2. Les techniques d'authentification

L'authentification permet à une personne de prouver son identité. Plusieurs techniques d'authentification sont possibles :

Authentification multiforme	Plusieurs niveaux d'authentification peuvent être utilisés en complément les uns des autres. <ul style="list-style-type: none"> • Le premier niveau est un mot de passe. • Le deuxième niveau est un objet (une clé USB ou un jeton d'authentification, par exemple). • Le troisième niveau est associé à la biométrie (empreinte ou analyse rétinienne).
Authentification par clé	Une paire de clés est générée. L'utilisateur conserve sa clé privée et envoie sa clé publique au serveur. Cette technique permet de se connecter à un serveur à distance sans utiliser de mot de passe.
Authentification unique (SSO, Single Sign-On)	Cette technique permet d'accéder à de multiples services au sein de l'entreprise avec un système d'authentification unique. Les avantages de cette méthode sont la simplicité et le gain de temps car les identifiants sont renseignés une seule fois en début de session pour accéder à plusieurs services.

3. Les techniques d'obtention des preuves

Les journaux systèmes (*logs*) sont des fichiers qui conservent l'historique des opérations liées à l'utilisation d'un serveur ou d'une application. Ces fichiers indiquent les actions réalisées (consultations, écritures, authentifications, etc.) en précisant la date, l'heure et l'adresse IP concernée. Ils peuvent donc être utilisés comme des éléments de preuve dans le cadre d'une procédure judiciaire.

La sécurité des applications Web

I

L'enjeu de la sécurité des applications Web

Les applications Web sont partout et doivent faire l'objet d'une grande attention en matière de sécurité. Il y a en effet deux grands enjeux :

Le respect de la loi 	Beaucoup d'applications Web effectuent des traitements sur des données à caractère personnel. Or, le RGPD oblige les entreprises à assurer la sécurité des données personnelles qu'elles collectent (article 32 du RGPD sur l'obligation de garantir un niveau de sécurité adapté au risque).
La santé, la réputation et la survie de l'entreprise	Les risques qui pèsent sur les applications Web peuvent entamer la santé économique et financière de l'organisation. La réputation de cette dernière peut être dégradée, avec des effets possibles sur sa pérennité. (►  Fiche savoirs CEJMA 3, p. 69).

II

Les risques et les menaces sur les applications Web

Les risques	Exemples de menaces
La brèche de confidentialité	Accès illégitime à des informations confidentielles (DCP, fichiers de configurations du serveur Web) suite à l'utilisation d'un mot de passe trop faible sur une page d'authentification ou à cause d'une injection SQL
L'atteinte à l'intégrité	Modification malveillante de la base de données d'un site Web.
L'ajout d'un code malveillant dans l'application Web	Un composant utilisé pour le développement n'est pas à jour et un attaquant exploite cette vulnérabilité pour compromettre le site Web en ajoutant un code malveillant.
Le risque de suppression de données	Permissions trop larges accordées à une personne utilisant des droits non nécessaires à son travail pour supprimer des comptes utilisateurs légitimes.
L'absence de traçabilité	Si les événements survenus sur un site (tentatives d'accès frauduleuses répétées sur une page d'authentification, par exemple) ne sont pas enregistrés dans les journaux systèmes, l'administrateur ne sera pas tenu au courant. Il ne pourra donc pas prendre des mesures correctives, ce qui peut encourager l'attaquant à poursuivre les tentatives.

III

La contre-mesure de codage sécurisé

La contre-mesure aux risques présentés passe par un codage sécurisé.

Exemple :

Application Web : formulaire d'enregistrement d'un nouveau client (nom et prénom).

Risque : brèche de confidentialité.

Menace : injection SQL. L'injection de code SQL dans un champ du formulaire peut permettre d'obtenir un succès d'authentification sans connaître le mot de passe.

Code injecté dans le champ du mot de passe : 'or 'a' = 'a. L'expression étant évaluée à vrai, le système valide l'authentification.

► Voir lexique BTS SIO, p. 221

...>

Les données saisies par l'utilisateur doivent faire l'objet d'une vérification car elles peuvent comporter du code malveillant. Le scénario de codage sécurisé est le suivant :

1. récupérer les données saisies ;
2. vérifier les données saisies : nombre de caractères et contenu avec une liste noire de caractères interdits (caractères typiques d'une injection SQL), tels que : /[]~!#{}|<> ;
3. traiter les données saisies si elles passent l'étape de la vérification de sécurité.

Exemple de code sécurisé :

```

1- <?php
2- //1-Récupération des informations saisies depuis le formulaire.
3- $ParamLogin = $_POST['login']; $ParamPassword = $_POST['password'];
4- //2-Vérification de la sécurité des données saisies.
5- var listeNoire = /[]~!#{}|<>;
6- $Validation = true;
7- if (Form.login.length > 15 || Form.password.length > 15)
8-   $Validation = false; //trop de caractères saisis, c'est suspect.
9- if (Form.login.value.search(listeNoire) ||
10-   Form.password.value.search(listeNoire)) > -1
11-   //Détection de caractères interdits, risque d'injection SQL.
12-   $Validation = false;
13- //3-Exécution de la requête si aucun problème de sécurité détecté.
14- if($Validation) {
15-   $requete = "SELECT * FROM CLIENT WHERE login = '$ParamLogin'
16-     and password='$ParamPassword';
17-   mysqli_query($requete); }
```

IV Les protocoles HTTP et HTTPS

Le protocole HTTP	HTTP est l'abréviation de <i>HyperText Transfer Protocol</i> (protocole de transfert hypertexte). C'est un protocole de communication développé pour le Web. Il n'est pas sécurisé car les informations transitent en clair sur le réseau. Le port d'écoute par défaut est 80.
Le protocole HTTPS	Il combine le HTTP avec une couche de chiffrement (TLS : <i>Transport Layer Security</i>). Ce protocole est utilisé pour les sites Web nécessitant de garantir la confidentialité des données. Le port d'écoute par défaut est 443.

La réglementation en matière de lutte contre la fraude informatique

I**Définition**

La fraude informatique consiste à falsifier des données stockées, en traitement ou en transit, afin d'en retirer des avantages personnels ou des gains financiers. La fraude informatique est un délit.

II**La réglementation**

Avec le développement du numérique, le système judiciaire a dû s'adapter aux nouvelles infractions commises et mettre en place des lois. En matière de fraude informatique, la réglementation suivante s'applique :

La loi Informatique et libertés du 6 janvier 1978

Elle introduit la notion de système de traitement automatisé de données.

Elle est complétée par la **loi Godfrain** du 5 janvier 1988 qui réprime les actes de criminalité informatique et de piratage. Les dispositions de la loi Godfrain sont intégrées dans le Code pénal livre III, sur les crimes et délits contre les biens.

La convention sur la cybercriminalité de 2001

Elle permet l'harmonisation des législations des États membres de l'UE et l'ajout d'infractions, telles que les fraudes liées à la propriété intellectuelle ou les atteintes à la confidentialité, l'intégrité et la disponibilité des systèmes informatiques.

Elle a été ratifiée en France par la **loi du 19 mai 2005**.

La loi pour la confiance dans l'économie numérique de 2004

Elle réprime le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions informatiques prévues par la loi.

Cette loi permet l'inclusion des données informatiques dans la liste des pièces pouvant être perquisitionnées dans le cadre des affaires de cybercriminalité.



Important ! Les entreprises ont une obligation légale de notification en cas de faille de sécurité ([Fiche Savoirs CEJMA 7, p. 125](#)).

III

Les principales infractions

D'après l'**ANSSI**, les infractions suivantes figurent parmi les plus répandus :

Production de faux et usage de faux	Les outils informatiques permettent de produire de faux documents beaucoup plus facilement qu'autrefois.
Vol de coordonnées bancaires via le phishing	Le <i>phishing</i> (ou hameçonnage) est une technique qui utilise l'envoi de courriels ciblés contenant des liens associés à un code malveillant.
Fraude spécifique à certains métiers	Il s'agit d'un détournement des avoirs de clientèles ou de la création de fausses opérations (par exemple, dans le domaine de la finance ou de la comptabilité).
Usurpation d'identité	Vol d'un mot de passe afin de prendre l'identité d'un tiers ou d'élever ses priviléges.
Accès ou maintien dans un système de traitement automatisé	Utilisation d'un code malveillant permettant de contourner la sécurité d'un système ou d'une application en vue de compromettre la confidentialité ou l'intégrité des données.
Attaque par ransomware	Il s'agit de chiffrer le disque de la victime et de demander une rançon en contrepartie du déchiffrement.
Arnaque aux faux supports techniques	Elle s'effectue par le biais de courriels signalant un faux problème technique ou une fausse opération de maintenance : une authentification est demandée à l'utilisateur via une page frauduleuse, qui récupérera les informations saisies par ce dernier.

IV

Les sanctions

Les dispositions de la loi Godfrain prévoient des peines pouvant aller de deux à dix ans d'emprisonnement selon que l'infraction est commise ou non en bande organisée. Le montant de l'amende dépend de la décision de justice rendue.

Code pénal	Infractions	Sanctions
Article 323-1 à 323-7	Atteintes aux STAD (systèmes de traitement automatisé de données)	Deux ans d'emprisonnement et 30 000 euros d'amende
Article 226-16	Procéder ou faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévue par la loi.	Cinq ans d'emprisonnement et 300 000 euros d'amende
Article 313-1	Escroquerie	Cinq ans d'emprisonnement et 375 000 euros d'amende
Article 2226-14-1	Usurpation d'identité	Un an d'emprisonnement et 150 000 euros d'amende

1 QCM



Retrouvez ce QCM
en version interactive
www.lienmini.fr/6988-602

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 de 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 une 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 Déborah déchiffre le message avec sa clé publique.
- Jean chiffre le message avec sa clé publique et Déborah déchiffre le message avec sa clé privée.
- Jean chiffre le message avec la clé publique de Déborah, et Déborah 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 pour 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



➤ Fiche savoirs technologiques 8

- 1 Relevez les principaux enjeux associés à l'archivage numérique.
- 2 Indiquez quels sont les domaines d'un système d'information mobilisés lors de la mise en œuvre d'une procédure d'archivage numérique.
- 3 Pourquoi la mise en place d'une veille technologique sur les supports d'archivage est-elle nécessaire ? Justifiez votre réponse.



Annexe

Les documents de référence du SI de l'État sur l'archivage numérique

Le développement des technologies de l'information et de la communication a profondément modifié les méthodes de travail en facilitant et en accélérant considérablement la production, le partage et le stockage d'informations numériques. En parallèle, la reconnaissance de l'écrit électronique comme preuve en 2000 a ouvert la voie à l'administration électronique, à la dématérialisation des processus métier et à la production d'originaux numériques. [...]

Les données numériques sont par nature très vulnérables pour deux raisons principales : d'une part, elles sont facilement manipulables et falsifiables. On rencontre également des difficultés à identifier la version validée d'un document et à avoir accès à l'information pertinente, nécessaire à la prise de décision. D'autre part, le support et le contenu de l'information ne sont plus indissociables, ce qui entraîne des conséquences majeures. En effet, l'affichage d'une information numérique est le résultat d'une harmonie entre systèmes logiciels, systèmes matériels, systèmes d'exploitation et périphériques. Ils sont tous soumis à des rythmes différents et de plus en plus rapides qui entraînent un risque d'obsolescence technologique. [...]

L'archivage numérique est donc un processus dynamique qui commence dès la création des documents. Il s'agit d'une fonction multi-facette qui fait appel à différents domaines entrant dans les schémas directeurs informatiques des organisations tels que :

- la gestion et la recherche documentaires (GED, bases de connaissance, moteurs de recherche, sémantique basée sur des référentiels, thesaurus, ontologies...) ;
- la preuve et la sécurité (empreintes, signature électronique, horodatage, gestion du cycle de vie de l'information, gestion des droits d'accès, gestion des traces), l'interopérabilité (entre systèmes basés sur des protocoles de communication et des formats d'échanges) ;
- les infrastructures de stockage ;
- le choix d'outils très pointus ciblés sur la conservation sur le long terme du numérique (outils d'identification et de conversion de formats, veille technologique sur les supports et les formats de données, plans de migrations des supports, des formats).

[https://references.modernisation.gouv.fr/
archivage-numerique](https://references.modernisation.gouv.fr/archivage-numerique)

3

Identifier les risques liés à une procédure d'authentification



›  Fiches savoirs technologiques 9 et 10

Situation

SortieFacile est un réseau social centré sur l'organisation de sorties thématiques (théâtre, expositions, balades...). Chaque membre du site décrit son profil et peut organiser des sorties auxquelles les autres membres peuvent s'inscrire. Le site vient d'être mis en ligne, et un de ses membres signale un incident via un courriel destiné au gérant.

- 1 Recherchez des informations sur Internet afin d'expliquer en quoi consiste un certificat de sécurité.
 - 2 Expliquez le message d'avertissement qui apparaît dans le courriel (annexe).
 - 3 Relevez, en justifiant, les risques encourus lors de l'authentification d'un membre sur ce site.
 - 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 ?

Annexe

Le courriel reçu par le gérant de SortieFacile

4 Caractériser les conséquences d'une fraude informatique



- > Fiche savoirs technologiques 3, p. 26
- > Fiche savoirs CEJMA 8

Situation

Vous participez à une session de formation sur la prévention les risques associés aux fraudes informatiques. La première partie de cette formation sera consacrée à l'étude des principales fraudes que l'on peut rencontrer au quotidien. La seconde partie se déroulera sous la forme d'un jeu sérieux afin d'examiner un exemple de fraude très répandue.

1^{re} partie Les principales fraudes informatiques

- Le site cybermalveillance.gouv.fr publie un kit de sensibilisation aux questions de sécurité du numérique dans lequel sont décrites les principales fraudes informatiques.
- 1 Rendez-vous sur le site cybermalveillance.gouv.fr et cliquez sur Accéder au kit.**
=> Site cybermalveillance.gouv.fr : www.lienmini.fr/6988-603
 - 2 Visionnez les vidéos associées à chacune des fraudes : hameçonnage, arnaque au faux support technique, rançongiciels. Complétez ensuite ce tableau.**

Fraudes	Descriptions > <i>En quoi consiste la fraude ?</i>	Conséquences > <i>Quelles conséquences pour l'entreprise victime ?</i>
Hameçonnage		
Arnaque au faux support technique		
Rançongiciels		

2^{de} partie Un jeu pour examiner la fraude de type «arnaque au président»

- 3 Visionnez la vidéo, puis expliquez en quoi consiste la fraude présentée.**
- 4 Expliquez le risque financier qui pèse sur l'entreprise cible.**
- 5 Classez ce risque en fonction du niveau de gravité et de vraisemblance.**
- 6 Les informations sur l'entreprise cible ont-elles été obtenues de manière légale ? Justifiez votre réponse.**
- 7 Quelle sanction encourt l'auteur de la fraude ?**

VIDÉO

Jeu sérieux sur l'arnaque au président

[www.lienmini.fr/
6988-604](http://www.lienmini.fr/6988-604)

Archiver et protéger les données et les preuves numériques

COMPÉTENCES

- Organiser la collecte et la conservation des preuves numériques
- Appliquer les procédures garantissant le respect des obligations légales

SAVOIRS ASSOCIÉS

- Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique
- Les organisations de lutte contre la cybercriminalité

Situation professionnelle

Cibeco a décidé de déposer plainte à la suite de l'attaque subie par son client Ecotri. Yaël et Sarah Darmon, les gérantes de Cibeco, ont poursuivi des investigations en vue de collecter des preuves numériques pour appuyer la plainte. Ces investigations ont permis de suspecter plusieurs menaces de sécurité qui les inquiètent.

Dans un premier temps, elles décident de procéder à la vérification de toutes les procédures de collecte et de conservation des preuves afin d'étudier leur exploitabilité. Dans un second temps, elles réalisent un audit technique pour s'assurer que les procédures prévues par Cibeco en cas de brèche de sécurité respectent bien les obligations légales.



➤ Voir présentation générale, p. 135

Missions professionnelles

1

Organiser la collecte et la conservation des preuves numériques

[PREUVES]



À la suite des attaques subies par Cibeco et Ecotri, Sarah Darmon souhaite savoir si des traces laissées par ces intrusions pourraient être exploitables dans le cas d'une enquête judiciaire. Elle vous charge de réaliser un audit technique sur la collecte et la conservation des preuves numériques au sein de la pépinière.

Travail à faire

- 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.
 - > Fiches savoirs technologiques 2 (p. 25) et 11
 - > Documents 1 à 4
- Relevez les événements collectés par les journaux systèmes de Cibeco et vérifiez que cette liste est bien complète.
 - > Fiches savoirs technologiques 2 (p. 25) et 11
 - > Documents 1 à 3
- Montrez que chacun des supports de stockage utilisé par Cibeco permet de conserver durablement les preuves collectées.
 - > Fiche savoirs technologiques 11
 - > Document 5
- 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.
 - > Fiche savoirs technologiques 11
 - > Document 6

Dossier documentaire

Document 1 Votre entretien avec la gérante de Cibeco au sujet de la gestion des preuves

Vous : J'ai besoin de savoir si, en cas d'attaque informatique, la pépinière est en mesure de fournir des éléments de preuve permettant d'appuyer une plainte. Comment est organisé votre système informatique pour pouvoir gérer ce type d'incident ?

S. Darmon : Nous disposons d'un serveur de centralisation des journaux systèmes qui trace toutes nos activités informatiques. Ces journaux servent de preuves en cas de besoin. Depuis l'attaque subie par notre client Ecotri, nous avons augmenté considérablement nos capacités de stockage.

Vous : Pouvez-vous en dire plus sur ce serveur de centralisation ?

S. Darmon : Il s'agit d'une grappe de deux serveurs redondés, située dans la salle des serveurs, qui collecte en temps réel les journaux systèmes de tous les serveurs de la pépinière et de nos clients. Si un serveur tombe en panne, le second prend le relais automatiquement.

Vous : Et concernant l'horodatage ?

S. Darmon : Nous disposons, en plus, d'un serveur de temps qui garantit que tous nos serveurs, ainsi que ceux de nos clients, sont à l'heure exacte.



Vous : Que collectez-vous dans vos journaux systèmes ?
S. Darmon : Tout ce que nous trouvons utile, notamment suite aux dernières cyberattaques, c'est-à-dire les accès aux ressources et les activités de nos systèmes.
Vous : Comment organisez-vous cette collecte ?
S. Darmon : Nos journaux systèmes sont collectés sur des grappes de disques configurés en RAID 5. Le tout est dans une baie spécifique dotée d'une climatisation et d'une alimentation redondante. L'accès à cette baie nécessite une clé.

Vous : Et pour la conservation à long terme ?

S. Darmon : Chaque fin de semaine, les journaux sont compressés et conservés sur des bandes magnétiques en double. De nouveaux fichiers sont alors créés sur les disques pour accueillir les journaux de la nouvelle semaine.

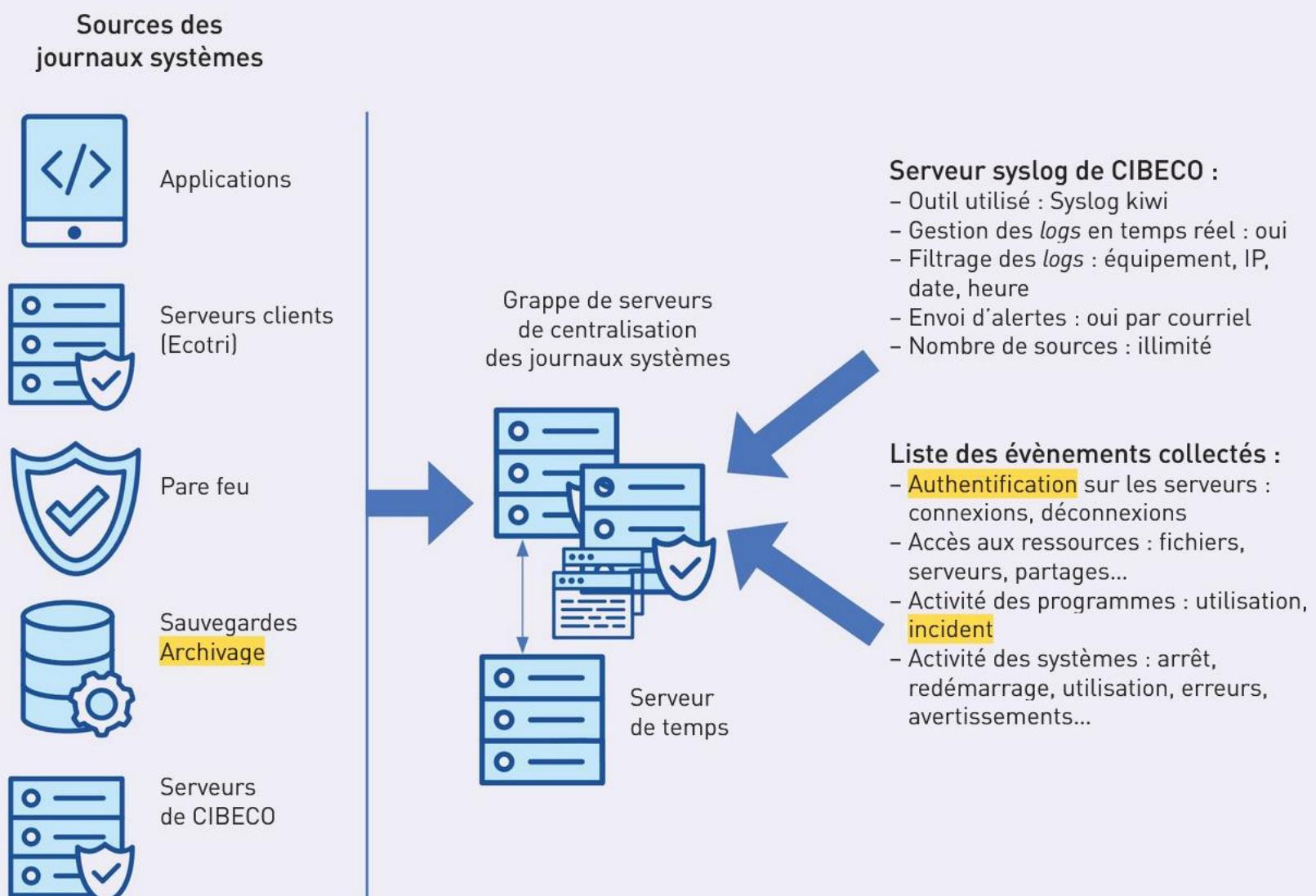
Vous : Puis-je avoir le détail des configurations dont nous venons de discuter ?

S. Darmon : Oui, je demande à Yaël de vous fournir des fiches techniques précises sur chacun de ces éléments.

Document 2

Le réseau de collecte des preuves numériques de Cibeco

La collecte des preuves s'appuie sur l'enregistrement des journaux systèmes. Un réseau dédié à cette collecte s'appuie sur trois serveurs : deux serveurs pour centraliser les journaux systèmes et un serveur de temps pour assurer un horodatage précis.



• La séparation des flux

La collecte des journaux systèmes s'effectue sur le **VLAN SERVEUR** via un réseau dédié séparé des autres réseaux utilisés par Cibeco et ses clients.

• La bande passante

Une bande passante minimale est garantie pour les flux de collecte des journaux systèmes via un mécanisme de

priorisation des flux. Cette bande passante minimale est configurée sur le pare-feu de Cibeco. Elle est conçue de sorte qu'au moins 10 % de la bande passante totale soit garantis pour le transit des journaux vers le serveur de centralisation, quel que soit le niveau de trafic sur le réseau.

➤ Voir lexique BTS SIO, p. 221

Missions professionnelles

Document 3 La configuration de la collecte des preuves par Cibeco

- Yaël Darmon vous fournit un extrait de la configuration des niveaux de traces enregistrés sur les serveurs de centralisation. Cette configuration dépend des événements collectés par les serveurs de la pépinière et de ses clients.

Événement tracé	Code de collecte configuré
Succès d'authentification sur la page du forum du client Ecotri	 INFORMATION
Plusieurs échecs d'authentification répétés pour déverrouiller l'accès aux archives de Cibeco	 AVERTISSEMENT
Arrêt inopiné du serveur de base de données contenant les données des clients d'Ecotri	 ERREUR
Inaccessibilité du site Web du client Ecotri	 ALERTE CRITIQUE

- Suite aux attaques informatiques récentes, l'entreprise a configuré une supervision de l'espace de stockage disponible pour l'enregistrement des journaux systèmes. Yaël Darmon a programmé la notification automatique d'une alerte lorsque le taux de remplissage des disques dépasse 75 %.

Taux de remplissage des disques	Notifications	Destinataires
> 75 %	Affichage d'un avertissement sur le tableau de bord de l'outil Syslog Kiwi	Yaël et Sarah Darmon
> 90 %	Envoi automatique d'un courriel d'alerte	

Document 4 Un exemple de consultation de preuves collectées par Cibeco

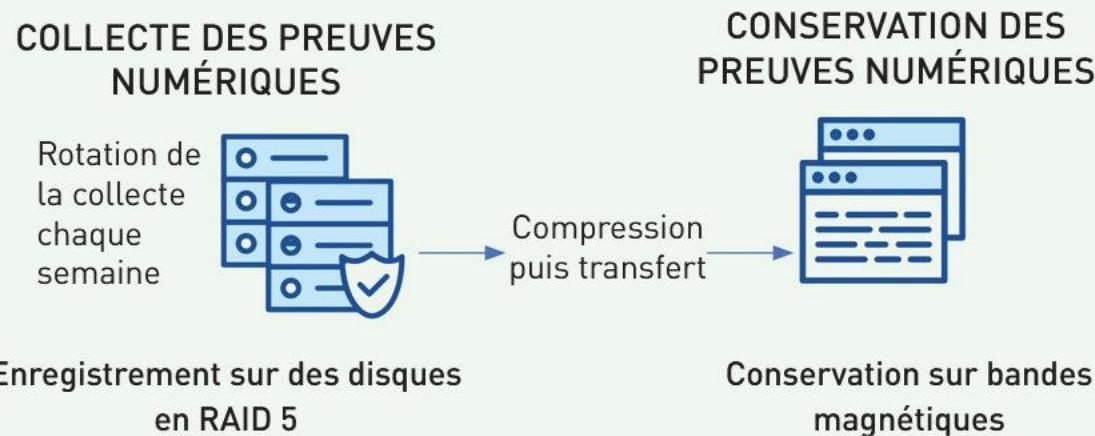
Le tableau de bord de l'application Syslog Kiwi pour la gestion des journaux systèmes permet de faire des recherches sur des événements passés à l'aide de filtres : date, adresse IP, serveur, etc.

Date	Heure	Priorité	Adresse IP	Message
09-06-2019	16:44:54	System4.info	82.54.99.66	Utilisateur jdupont connecté au forum du client Ecotri
09-06-2019	19:44:51	Local5.Alert	99.23.14.67	Inaccessibilité du site Web d'Ecotri

➤ Voir lexique BTS SIO, p. 221

Document 5 La conservation des preuves numériques par Cibeco

- Chaque fin de semaine, les preuves collectées dans les journaux systèmes sont extraites automatiquement des disques puis sont compressées en vue de leur transfert sur des bandes magnétiques dans une baie de stockage climatisée et verrouillée. La nouvelle collecte peut écraser la collecte de la semaine précédente sur les disques, et ainsi de suite. La salle des serveurs qui abrite cette baie est dotée d'un système anti-incendie, installé récemment.



- Le système de conservation utilisé par Cibeco présente les caractéristiques suivantes :

Caractéristiques de conservation	Valeurs
Nombres de bandes disponibles	10
Capacité de stockage par bande	10 To
Copie en double	OUI
Politique de nommage des fichiers de journaux conservés	Nom indiquant la date de création Exemple : Logs_18112019

Document 6 Le lieu de conservation des preuves numériques

La baie utilisée par Cibeco pour collecter et conserver les éléments de preuves numériques se situe dans la salle des serveurs S02 du bâtiment A.

Bâtiment A	Salle des serveurs avec baie de conservation des preuves numériques
Bâtiment B	Uniquement des bureaux. Liaison fibre avec le bâtiment A

Missions professionnelles

2

Appliquer les procédures garantissant le respect des obligations légales

Suite à l'audit technique réalisé après l'attaque du site Web du client Ecotri, plusieurs brèches de sécurité sont suspectées et signalées dans des feuilles de révélation et d'analyse des problèmes (FRAP). Ces fiches vous sont remises afin que vous puissiez vérifier si les procédures prévues pour faire face aux brèches de sécurité suspectées respectent bien les obligations légales.



Travail à faire

Le premier point qui ressort de l'audit concerne la **confidentialité** des accès aux ressources informatiques de Cibeco.

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.

- Fiches savoirs technologiques 2, 9 (pp. 25 et 151) et 11
➤ Documents 1 et 2

Le deuxième point relevé par l'audit concerne la procédure de transfert des journaux systèmes des disques vers les bandes magnétiques.

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 .

- Fiches savoirs technologiques 2, 9 (pp. 25 et 151) et 11
➤ Documents 1 et 3

La troisième FRAP concerne le **risque** lié à l'indisponibilité des applications des clients de la pépinière.

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.

- Fiches savoirs technologiques 2 (p. 25) et 11
➤ Documents 1 et 4

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

- Fiche savoirs CEJMA 9
➤ Document 1

➤ Voir lexique BTS SIO, p. 221

Dossier documentaire

Document 1 Entretien sur les procédures de gestion des incidents chez Cibeco

Y. Darmon : Nous venons de terminer l'audit technique sur nos procédures en cas de brèche de sécurité.

S. Darmon : Qu'en est-il exactement ?

Y. Darmon : J'ai relevé plusieurs problèmes potentiels qui pourraient impacter la confidentialité, l'intégrité et la disponibilité de nos systèmes. J'ai notifié sur des FRAP tous ces problèmes potentiels en indiquant les procédures prévues actuellement pour y faire face s'ils venaient à se concrétiser.

S. Darmon : Nous avons donc encore des problèmes potentiels... Je ne m'y attendais pas, nous avons tellement investi après l'intrusion dans nos archives. Notre système de traçabilité Syslog Kiwi a coûté cher, sans compter tous nos efforts pour augmenter nos capacités de stockage.

Y. Darmon : C'est vrai, notre analyse montre que nous disposons de bons outils pour conserver les preuves en cas d'intrusion. Mais posséder ces outils ne suffit pas. Il faut appliquer correctement les procédures qui vont avec. Il y a des lois à respecter et il faut absolument vérifier que les procédures prévues dans nos

FRAP répondent aux obligations légales qui s'imposent.

S. Darmon : Nos procédures en cas d'incidents ne sont donc pas valables ?

Y. Darmon : C'est ce qu'il faut vérifier. J'ai relevé trois FRAP représentatives. Par exemple, je m'interroge sur la procédure de transfert de nos journaux systèmes sur bandes... Car si l'analyse montre que la collecte est conforme aux recommandations d'usage, il y a peut-être un risque pour l'intégrité au moment du transfert. Or, la loi impose une garantie de cette intégrité.

S. Darmon : Et les deux autres ?

Y. Darmon : Si la confidentialité de nos clés d'administration des serveurs est compromise, notre procédure de secours est sans doute insuffisante. De plus, certains de nos serveurs ne sont pas redondés. Nous avons bien des serveurs de secours, mais leur configuration ne garantit peut-être pas une reprise de la disponibilité totale pour nos clients.

S. Darmon : Il y a urgence. Notre technicien doit faire un bilan de tout cela immédiatement.

Document 2 Extrait de la FRAP n° 1 sur la procédure de secours pour l'accès aux serveurs

FRAP n° 1 Procédure de secours pour l'accès à distance aux serveurs	
Problème	L'accès à distance aux principaux serveurs de Cibeco nécessite une authentification par clé. Seules les personnes habilitées ont connaissance des clés. Celles-ci sont présentes uniquement sur les ordinateurs portables de Yaël et Sarah. Dans ce scénario, on envisage la perte de ces ordinateurs portables.
Procédure prévue (faits, constats)	Dans le scénario envisagé, la procédure suivante est prévue : 1. génération de nouvelles clés par Sarah directement depuis les serveurs. Une seule et même clé permet l'accès à tous les serveurs en mode administrateur; 2. copie du fichier contenant la nouvelle clé sur une clé USB déposée sur le bureau de Yaël, avec un post-it indicatif ; 3. confirmation de la réception de la nouvelle clé par Yaël.
Détail de la procédure	– Suppression des anciennes clés : non. – Chiffrement du disque de l'ordinateur portable et de la clé USB : non. – Effacement sécurisé de la clé USB : non.

➤ Voir lexique BTS SIO, p. 221

Missions professionnelles

Document 3 Extrait de la FRAP n° 2 sur l'exploitation des journaux systèmes suite à une fraude

FRAP n° 2 Procédure d'exploitation des journaux systèmes suite à une fraude	
Problème	Cibeco soupçonne des tentatives d'accès frauduleuses à ses serveurs et compte mettre à profit les journaux systèmes pour compromettre la personne malveillante.
Procédure prévue (faits, constats)	Dans le scénario envisagé, la procédure de conservation et de consultation des journaux systèmes utilisés est la suivante : 1. collecte des journaux systèmes sur des disques ; 2. transfert des journaux sur des bandes magnétiques ; 3. extraction des journaux avec un filtre en vue d'une suite judiciaire.
Détail de la procédure	La phase de transfert des journaux systèmes des disques vers les bandes magnétiques présente les caractéristiques suivantes : – transit par le réseau de Cibeco : oui ; – compression : oui ; – chiffrement : non ; – vérification des sommes de contrôles : non.

Document 4 Extrait de la FRAP n° 3 sur la panne d'un serveur Web d'un client

FRAP n° 3 Panne d'un serveur Web d'un client	
Problème	Le serveur Web d'un client tombe en panne.
Procédure prévue (faits, constats)	Dans le scénario envisagé, la procédure de dépannage est la suivante : 1. chaque serveur Web d'un client fait l'objet d'une sauvegarde tous les trois mois ; 2. après une panne, cette sauvegarde est injectée dans un serveur de secours via une copie en temps différé ; 3. le serveur de secours est mis en production afin de restaurer l'accès des clients.
Détail de la procédure	La sauvegarde des serveurs Web des clients présente les caractéristiques suivantes : – copie des pages Web : oui, une fois par trimestre ; – copie de la base de données associée au site Web : oui, une fois par trimestre.

Organiser la collecte des preuves numériques

›  Fiche savoirs technologiques 11



Afin de réduire ses coûts, Cibeco souhaite s'orienter vers un nouveau pare-feu *open source*. La solution pfSense semble intéressante, mais il faut la tester avant de la valider.

À partir des machines virtuelles utilisées pour le travail en laboratoire du chapitre 6, vous effectuerez des configurations permettant de valider les moyens de preuves numériques offerts par cette solution. Deux types de tests sont à réaliser :

- d'abord, la configuration d'un serveur de temps : vous configurez un serveur de temps afin de garantir que toutes les preuves collectées par le pare-feu pfSense indiquent une heure exacte ;
- ensuite, la configuration de la collecte des traces : vous configurez sur pfSense l'enregistrement des traces des clients qui se connectent au serveur Web Mutillidae.

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

ÉTAPE 2 La configuration du serveur de temps sous pfSense

3. Mettez votre pare-feu pfSense à l'heure.
›  Document 3
4. Configurez votre pare-feu pfSense pour qu'il soit un serveur de temps.
›  Document 4
5. Mettez le serveur Web Mutillidae à l'heure en vous appuyant sur le serveur de temps pfSense.
›  Document 5

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.
›  Document 6
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.
›  Document 7

Document 1 La préparation de l'environnement de travail

Pour préparer l'environnement de travail :

- si vous avez effectué le travail en laboratoire du chapitre 6, vous pouvez passer directement à la question n° 2 du travail à faire ;
- si vous n'avez pas effectué le travail en laboratoire du chapitre 6, vous devez configurer l'environnement de travail initial en suivant les procédures décrites dans l'étape 1 du travail en laboratoire du chapitre 6, p. 145.

Document 2 La procédure de connexion au pare-feu

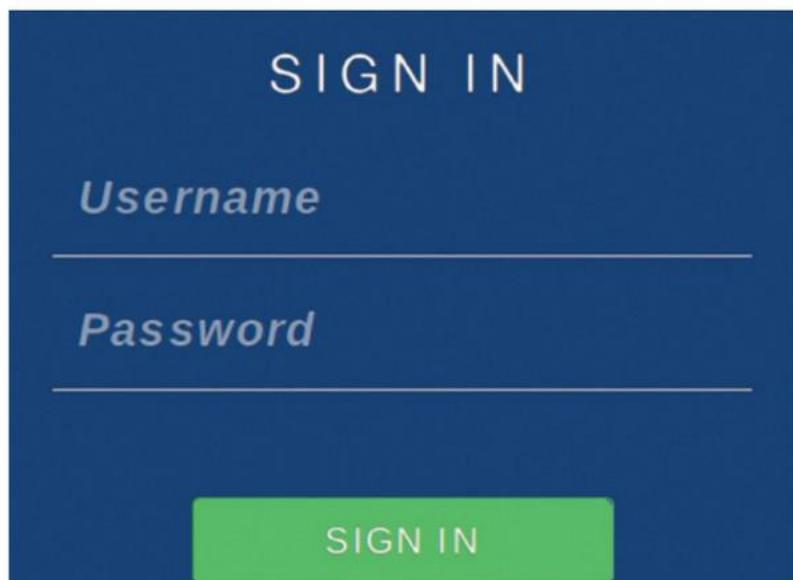
Afin de disposer d'un horodatage correct lors de la collecte des journaux systèmes servant de preuves, il est nécessaire que le serveur Web Mutillidae soit à l'heure (voir Fiche savoirs technologiques 11). Dans la maquette utilisée, c'est le pare-feu pfSense qui joue le rôle de serveur de temps. Les autres serveurs se mettent à l'heure en interrogeant le serveur de temps sous pfSense. Pour se connecter au pare-feu pfSense, il faut suivre la procédure suivante :

Depuis la machine **DELAGRAVE-CLIENT-LEGITIME-UBUNTU** :

Ouvrir le navigateur et utiliser l'URL ci-dessous afin de se connecter au pare-feu :

https://192.168.50.254

L'adresse IP indiquée correspond à celle du pare-feu sur l'interface servant de passerelle pour les machines clientes du réseau **LAN-IN** (voir le schéma du réseau, p. 145). Par défaut, l'authentification sur le pare-feu pfSense se fait avec l'identifiant **admin** et le mot de passe **pfsense**.



Document 3 La mise à l'heure du pare-feu

Il convient de s'assurer que le pare-feu est configuré sur le bon fuseau horaire. Pour cela, il faut :

- d'abord, aller dans le menu **System**, puis cliquer sur **General Setup**.
- ensuite, dans la rubrique de localisation, sélectionner la zone géographique **Europe/Paris** ;
- enfin, valider en cliquant sur **Save** en bas de l'écran.

Document 4 La configuration du serveur de temps sous pfSense

Lorsque le pare-feu pfSense est sur le bon fuseau horaire, il faut suivre une procédure pour le configurer comme un serveur de temps :

- d'abord, aller dans le menu Services, puis cliquer sur **NTP**;
 - ensuite, indiquer l'interface sur laquelle le **serveur de temps** écoute les requêtes de mise à l'heure ainsi que le **pool de serveurs sur Internet** (groupe de serveurs) permettant une mise à l'heure correcte.
- En ce qui concerne l'interface d'écoute du serveur NTP : il faut sélectionner l'interface SRV-IN. C'est sur cette interface que se situe la zone serveur du contexte. Ce réseau ne comporte qu'un seul serveur Web, qui héberge l'application Web Mutillidae.

• En ce qui concerne le **pool de serveurs sur Internet**, il s'agit d'un fonctionnement par strates. Le serveur Web qui héberge Mutillidae se met à l'heure via le serveur de temps du pare-feu pfSense, qui, lui-même, se met à l'heure exacte en consultant d'autres serveurs de temps présents sur Internet dans le pool sélectionné. C'est pourquoi votre pare-feu pfSense doit avoir accès à Internet. Dans votre laboratoire, il suffit de laisser la valeur proposée par défaut à **0.pfsense.pool.ntp.org**. Enfin, cliquer sur **Save** en bas de l'écran. Votre pare-feu fait désormais office de serveur de temps.

Document 5 La mise à l'heure du serveur Web Mutillidae

Lorsque le serveur de temps pfSense est à l'heure, vous pouvez l'utiliser pour mettre à l'heure votre serveur Web Mutillidae. La procédure à suivre est la suivante :

Depuis la machine **DELAGRAVE-SERVEUR-UBUNTU** :

- ouvrir le fichier **ntp.conf** localisé dans le répertoire **/etc** avec la commande **sudo nano /etc/ntp.conf**;
- dans ce fichier, supprimer toutes les lignes commençant par **pool** et les remplacer par la seule ligne suivante :**server 172.16.10.254**;

- enregistrer le fichier, puis quitter l'éditeur de texte nano. L'adresse IP indiquée est celle du pare-feu, donc du serveur de temps;
- redémarrer le service avec la commande **sudo service ntp restart**;
- utiliser la commande **ntpq -pn** afin de vérifier que l'adresse IP de votre serveur de temps s'affiche.

Document 6 La configuration de la collecte des traces

Pour que le pare-feu pfSense enregistre les traces des connexions des clients au serveur Web Mutillidae, il faut éditer une règle de filtrage. La procédure à suivre est la suivante :

Depuis la machine **DELAGRAVE-CLIENT-LEGITIME-UBUNTU** :

- - d'abord, se connecter au pare-feu via le navigateur Web et cliquer sur le menu **Firewall**, puis sur **Rules**;
- ensuite, cliquer sur l'interface **LAN_IN**, puis cliquer sur l'icône permettant de modifier la deuxième règle qui autorise l'accès au serveur Web Mutillidae (voir ci-contre). Une page permettant d'éditer la règle de filtrage s'ouvre. Aller en bas de la page et cocher la case permettant de tracer les événements associés à cette règle de filtrage :

Journal **Journaliser les paquets gérés par cette règle**

- enfin, valider en cliquant sur les boutons **Save** et **Apply Changes**. Tout accès au serveur Web Mutillidae depuis le réseau LAN-IN est maintenant tracé.

➤ Voir lexique BTS SIO, p. XXX

Document 7 Le test de collecte des journaux systèmes

Pour vérifier si une connexion au serveur Web Mutillidae est bien tracée à l'heure exacte, il faut effectuer les manipulations suivantes.

Depuis la machine **DELAGRAVE-CLIENT-HACKER-UBUNTU** :

- ouvrir le navigateur et se connecter à l'application Web Mutillidae en utilisant l'URL suivante : **http://172.16.10.5/mutillidae**. Il est inutile de s'authentifier. Il suffit de naviguer sur n'importe quelle page de l'application pour générer des traces ;
- ensuite, se rendre sur le pare-feu pour vérifier les traces collectées en réalisant le travail qui suit.

Depuis la machine **DELAGRAVE-CLIENT-LEGITIME-UBUNTU** :



- se connecter au pare-feu et cliquer sur le menu **Firewall**, puis sur l'interface **LAN_IN**. Ensuite, cliquer sur l'icône des journaux systèmes situé en haut, à droite de la page ;
- ensuite, utiliser un **filtre** permettant de tracer toutes les connexions à distance du serveur Web Mutillidae. L'icône de filtrage est située en haut, à droite de l'écran.



Les plans de secours, la traçabilité et l'audit technique

Le contrôle de la sécurité nécessite des outils permettant de prévoir un plan de secours, la traçabilité des événements ainsi qu'un audit technique des procédures prévues par l'organisation en cas de brèche de confidentialité, d'intégrité ou de disponibilité.

I

Les plans de secours

Le plan de continuité d'activité (PCA) et le plan de reprise d'activité (PRA) permettent aux organisations de poursuivre leur activité en cas d'incident ou de sinistre.

Plan de continuité d'activité	L'objectif est d'assurer la continuité des activités en cas d'incident. Un PCA peut, par exemple, prévoir des sauvegardes, qui permettent des restaurations en cas de pertes de données.
Plan de reprise d'activité	L'objectif est d'assurer la reprise des activités en cas de sinistre important (incendie, inondations, etc.). Par exemple, une entreprise peut prévoir un site de secours.

II

La traçabilité

La traçabilité permet de suivre les actions réalisées au sein d'un système informatique. Elles sont enregistrées dans des *logs* qui peuvent servir de preuves numériques. L'**ANSSI** recommande d'enregistrer les événements suivants :

Événements	Exemples
Authentification	Réussites et échecs d'authentification, utilisation des différents mécanismes d'authentification, élévation de priviléges.
Gestion des comptes et des droits	Ajouts, suppressions de comptes ou de groupes, affectations ou suppressions de droits aux comptes ou aux groupes, modifications des données d'authentification.
Accès ou modification des ressources et des configurations	Accès ou tentatives d'accès en lecture, écriture ou exécution aux ressources et aux applications. Réinitialisation de configurations.
Activité des processus (programmes) et des systèmes (matériels et systèmes d'exploitation)	Démarrages ou arrêts, dysfonctionnements, surcharges du système, chargement ou déchargement de modules, activité matérielle (défaillance, connexions, déconnexions).

Afin que l'exploitation juridique des preuves numériques soit garantie, l'**ANSSI** recommande également d'appliquer les procédures ci-dessous.

1. La conservation des traces

Les journaux systèmes doivent être collectés dans un format lisible et facilement consultable. Ils doivent faire l'objet d'un chiffrement et d'une compression. Il faut également prévoir un espace disque suffisant, redondé et supervisé afin de garantir la continuité de la collecte.

2. La centralisation et la rotation des traces

Les journaux systèmes doivent être centralisés afin d'éviter l'utilisation de plusieurs sources incohérentes. Il est nécessaire de prévoir un processus qui automatise la permutation, la suppression et l'envoi des journaux selon des intervalles de temps permettant une conservation pendant une certaine durée : trois mois pour les réseaux d'entreprise, et une année pour les fournisseurs d'accès à Internet.

➤ Voir lexique BTS SIO, p. 221

...>

3. L'horodatage

La collecte doit être effectuée avec des serveurs parfaitement à l'heure afin d'obtenir des informations exactes sur la date et l'heure. Le serveur de temps peut être utilisé pour synchroniser les horloges de l'ensemble des serveurs. Il s'appuie sur le protocole NTP (*Network Time Protocol*).

4. Le transfert en temps réel

L'enregistrement des événements doit être réalisé immédiatement, et non en temps différé, pour garantir qu'il correspond à la photographie exacte des faits enregistrés au moment de la consultation des traces.

5. Le réseau dédié

Afin de séparer les flux, il convient de faire transiter les journaux par un réseau dédié avec une bande passante minimale garantie.

III

L'audit technique

L'audit technique vise à évaluer les procédures prévues par une organisation en cas de brèche de sécurité. Cet audit s'appuie sur l'élaboration de FRAP (feuilles de révélation et d'analyse des problèmes). Ces documents sont complétés lorsque des dysfonctionnements ou des risques sont détectés : constat du problème, causes, conséquences, recommandations.

IV

Les outils de contrôle de la sécurité des critères DIC

Disponibilité	Utilisation de solutions de hautes disponibilités (<i>High Availability</i> , HA) permettant de garantir une continuité de service en cas de défaillance d'un serveur ou d'une application. Exemple : redonner un serveur pour l'accès à un service.
Intégrité	Utilisation d'algorithmes de sommes de contrôles, qui calculent un condensé unique à partir d'une information donnée. La moindre modification de contenu entraîne un changement du résultat de la somme de contrôle. Exemple : l'algorithme MD5 (<i>Message Digest 5</i>) ou le SHA-256 (<i>Secure Hash Algorithm</i>).
Confidentialité	Utilisation d'algorithmes de chiffrement récents et robustes. Exemple : l'algorithme AES (<i>Advanced Encryption Standard</i>), qui est approuvé par la NSA (<i>National Security Agency</i>) aux États-Unis.

Fiche savoirs CEJM appliquée 9

Les organisations de lutte contre la cybercriminalité

La recrudescence des actes de cybercriminalité a amené de nombreux États à mettre en place des organismes spécifiques afin de lutter contre ce phénomène. Par exemple, l'Union européenne dispose d'un centre destiné à coopérer avec l'ensemble des États membres. Les services de police et de gendarmerie des États possèdent des unités spécialisées selon le type de criminalité concerné.

I

L'Union européenne contre la cybercriminalité



Europol (European Police Office) est une agence européenne de police criminelle qui facilite l'échange de renseignements entre les polices nationales des États membres en matière de stupéfiants, de terrorisme, de criminalité internationale, de pédophilie et de cybercriminalité au sein de l'Union européenne.

Début des missions
1^{er} juillet 1999

Siège
La Haye (Pays-Bas)



Le Centre européen de lutte contre la cybercriminalité (*European Cybercrime Centre* ou EC3) est une structure luttant contre la cybercriminalité en Europe. Elle est située dans les locaux d'Europol. La création de ce centre fait partie des mesures prises par l'UE pour protéger les citoyens contre la criminalité en ligne : fraude, maltraitance infantile, activités illicites exercées par des organisations criminelles. Europol est à l'initiative, avec la police néerlandaise et les sociétés Kaspersky Lab et McAfee, de la plateforme No More Ransom, dont le but est d'aider les victimes des rançongiciels à retrouver leurs données chiffrées sans avoir à payer les criminels.

Début des missions
1^{er} janvier 2013

Siège
La Haye (Pays-Bas)



Eurojust (Unité de coopération judiciaire de l'Union européenne) est l'agence européenne chargée de renforcer la coopération judiciaire entre les États membres, par l'adoption de mesures destinées à promouvoir une coordination optimale des actions d'enquêtes et de poursuites.

Début des missions
28 février 2002

Siège
La Haye (Pays-Bas)

La lutte contre la cybercriminalité en France

En France, des services spécialisés sont chargés de la lutte contre la cybercriminalité.

La police nationale



La Sous-direction de lutte contre la cybercriminalité (SDLC) est un organisme de la police française voué à la lutte contre la cybercriminalité. C'est une branche de la Direction centrale de la police judiciaire.

La gendarmerie nationale



Le Centre de lutte contre les criminalités numériques (C3N) regroupe l'ensemble des unités du pôle judiciaire de la gendarmerie nationale qui traitent directement de la criminalité et des analyses numériques. Le C3N assure également l'animation et la coordination, au niveau national, de l'ensemble des enquêtes menées par le réseau des enquêteurs numériques de la gendarmerie.

La préfecture de police



La Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) est un service de la Direction régionale de la police judiciaire de Paris créé en février 1994. Sa mission essentielle est de lutter contre les atteintes aux systèmes de traitement automatisé de données (STAD), qu'il s'agisse des réseaux informatiques ou télématiques, ou des systèmes de télécommunications (GSM, autocommutateurs d'entreprises, etc.).

III La lutte internationale contre la cybercriminalité

Dans le reste du monde, d'autres organismes luttent contre la cybercriminalité. Aux États-Unis, le FBI (*Federal Bureau of Investigation*) est la principale agence fédérale chargée d'enquêter sur les cyberattaques.

Europol a créé le J-CAT (*Joint Cybercrime Action Taskforce*), une structure de coordination spécialement dédiée à la lutte contre la cybercriminalité dans l'Union européenne et au-delà.

1 QCM

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 de 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 contrôle (*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 du 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.



Retrouvez ce QCM
en version interactive
www.lienmini.fr/6988-701

2 Utiliser les journaux systèmes comme preuves numériques



› Fiche savoirs technologiques 11

› Fiche CEJMA 9

Situation

L'annexe ci-dessous présente deux cas concrets rencontrés dans le contexte d'un établissement scolaire. Répondez aux questions suivantes en vous reportant à cette annexe.

Cas n° 1

- 1 Indiquez si ce cas relève d'un acte malveillant. Justifiez votre réponse.
- 2 Expliquez en quoi la consultation des journaux systèmes a permis d'améliorer le fonctionnement du réseau informatique de l'établissement.

Cas n° 2

- 3 Indiquez si ce cas constitue une brèche de confidentialité sur les données à caractère personnel. Justifiez votre réponse.
- 4 Donnez le nom de l'organisme chargé d'enquêter. Indiquez qui est le responsable juridique du système d'information.
- 5 Justifiez la nécessité de consulter les journaux systèmes pour aider à la résolution de ce cas.

Annexe

Deux cas concrets



Cas n° 1

Les utilisateurs de l'établissement se plaignent du ralentissement de l'accès à Internet à une certaine heure de la journée. À la demande du chef d'établissement, la responsable informatique effectue une analyse volumétrique, à partir des journaux de consultation du Web et elle ne constate aucun transfert particulièrement volumineux à l'heure concernée. Elle poursuit ses investigations sur d'autres journaux des systèmes de l'établissement et finit par découvrir qu'il s'agit du processus de remontée de données du logiciel de gestion de parc informatique. Suite à ce constat, elle reconfigure le processus de remontée afin que ce dernier opère la nuit et tout rentre dans l'ordre.

Cas n° 2

Un élève a usurpé le compte d'un de ses camarades dans l'application Gibii (Gestion informatisée du brevet informatique et Internet). L'usurpateur a déposé, dans l'application, des insultes envers un professeur, qui a porté plainte. Pour les besoins de l'enquête, la gendarmerie demande au responsable juridique du système d'information (le chef d'établissement) les journaux informatiques, qui vont permettre d'innocenter le propriétaire du compte usurpé et de remonter à l'auteur du délit.

<https://eduscol.education.fr>

3 Exploiter des preuves numériques



- > Fiche savoirs technologiques 11
- > Fiche CEJMA 9

Situation



SA-Conseil fournit des prestations de conseil à de jeunes startups. L'entreprise propose, notamment, des activités de coaching et des sessions de formations dans le domaine de la gestion.

Récemment, SA-Conseil a été victime d'une attaque qui a remis en cause sa réputation. En effet, une photographie truquée avec le logo de l'entreprise et montrant le gérant en train de vomir a été publiée sur les réseaux sociaux. Très vite, le partage de cette photographie est devenu viral. Le gérant de SA-Conseil a déposé plainte.

Vous travaillez au sein du support technique de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et vous êtes chargé(e) d'enquêter sur la mise en ligne et la circulation de la photographie. Vous devez, notamment, effectuer des tests avec un outil d'investigation disponible sur Internet.

- 1** Rappelez quel est le rôle de l'OCLCTIC dans le cadre de cette affaire.
- 2** À l'aide de recherches sur Internet, définissez les termes suivants : métadonnées, données EXIF, géolocalisation.
- 3** Rendez-vous sur le site GitHub, qui contient des exemples d'images permettant de réaliser des tests pour retrouver des métadonnées :
 - > Site GitHub : www.lienmini.fr/6988-702
- 4** Ouvrez un autre onglet sur le navigateur et rendez-vous sur le site metapicz.com.
 - > Site metapicz : www.lienmini.fr/6988-703
- 5** Téléchargez une image depuis le site GitHub et importez-la dans la zone d'analyse du 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.
- 7** Expliquez l'intérêt de l'outil testé dans le cadre de l'enquête en cours.

4

Collecter des preuves numériques



› Fiche savoirs technologiques 11

- 1 Rendez-vous sur le site <https://www.sophos.com>, puis cliquez sur le lien permettant d'accéder aux démonstrations en ligne (<https://secure2.sophos.com/en-us/products/demos.aspx>).
- 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.
- 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.
- 4 Relevez les noms des colonnes du tableau de synthèse des journaux systèmes. Expliquez le rôle de chaque colonne.

Temps	Composants du journal	État	Nom d'utilisateur	IP source
Admin 2020-01-30 02:22:42	GUI	Successful	demo	176.144.76.59

- 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 ?

Admin

- 6 Dans la liste déroulante, sélectionnez la rubrique *Admin*, puis saisissez la chaîne de caractère *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.

Search...

Évaluation 4

L'organisation cliente

Fermabio est une entreprise familiale fondée en 2002 qui distribue des produits issus de l'agriculture biologique. Située à Nangis, dans le département de Seine-et-Marne, Fermabio s'appuie sur un solide réseau de producteurs locaux qui lui assurent un approvisionnement régulier en produits frais. Ses clients sont des magasins bio qui passent leurs commandes sur un site extranet comportant l'ensemble des produits proposés (fruits et légumes, boissons, épicerie, hygiène et beauté). L'accès à ce site nécessite une authentification via un identifiant et un mot de passe.

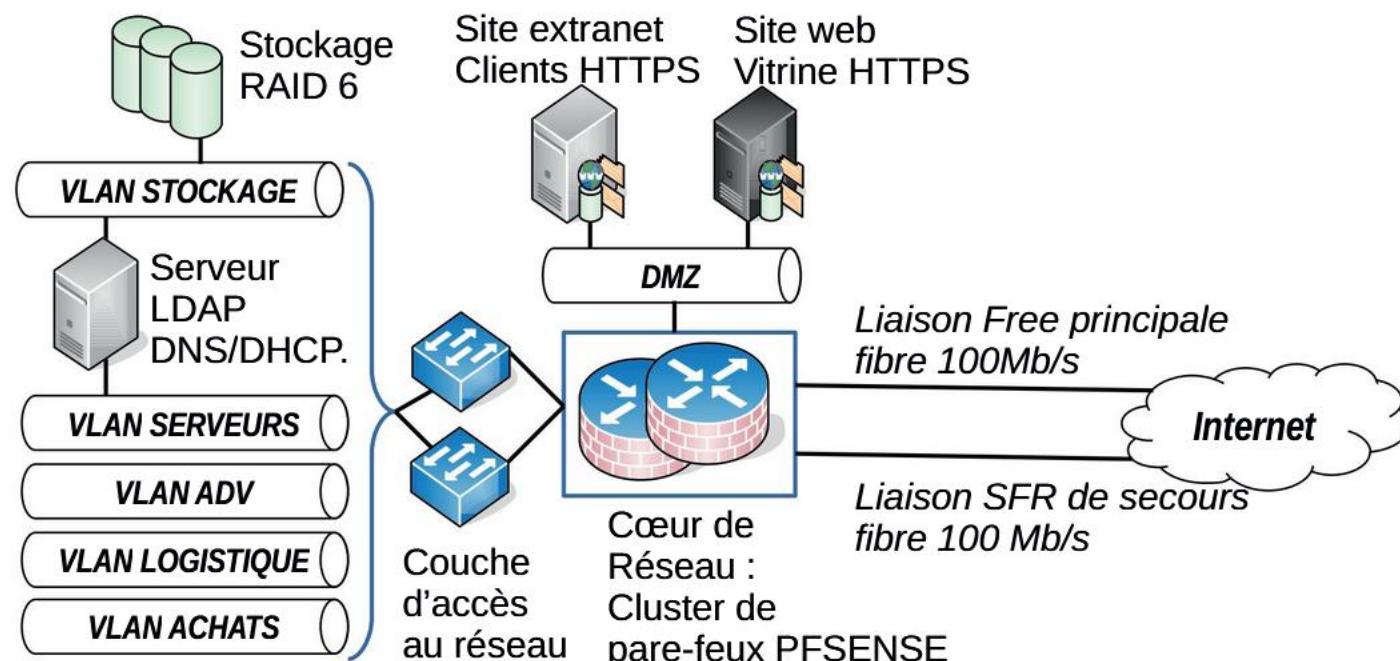
Fermabio possède un entrepôt de 4 000 m² situé près d'un bâtiment comportant les services de gestion suivants : administration des ventes (ADV), logistique et achat. Récemment, Fermabio a été victime d'une cyberattaque. Les comptes de plusieurs clients ont été piratés. L'attaque a été détectée tardivement suite aux plaintes des victimes. Après cette attaque, Fermabio a fait appel à la société Securenet, spécialisée en conseil sur la sécurité du numérique.



Le prestataire informatique

Securenet est une entreprise spécialisée en prestations d'audit sur la cybersécurité. Elle analyse les systèmes informatiques de ses clients et produit des rapports comportant des recommandations à suivre.

Architecture réseau de Fermabio



Votre mission

Vous êtes technicien(ne) informatique chez Securenet chargé(e) d'analyser la sécurité informatique du client Fermabio. Dans un premier temps, vous analysez la sécurité du site extranet de FERMABIO. Dans un second temps, vous menez une étude de la traçabilité des événements informatiques de Fermabio afin d'améliorer la réactivité en cas de cyberattaque.

Missions**1****Analyser la sécurité du site extranet de Fermabio**

Afin d'auditer la sécurité du site extranet, vous effectuez deux tests qui analysent le code source du site et le fichier de configuration du serveur Web.

- 1.1.** Expliquez pourquoi le test n°1 montre que la confidentialité et l'intégrité ne sont pas garanties.
- 1.2.** Proposez une modification de ce code source afin de corriger la vulnérabilité détectée.
- 1.3.** En vous appuyant sur le schéma du réseau de Fermabio, expliquez quelles sont les configurations qui garantissent une disponibilité du site extranet.
- 1.4.** Indiquez, en justifiant, si le résultat du test n° 2 révèle un problème de sécurité.

2**Améliorer la traçabilité des évènements informatiques de Fermabio**

La fraude subie n'a laissé aucune trace exploitable sur les serveurs et a été détectée tardivement par la comptabilité. Vous cherchez à comprendre cette anomalie en vérifiant les configurations d'enregistrement des journaux systèmes.

- 2.1.** Expliquez le problème posé par la configuration d'enregistrement des journaux systèmes de Fermabio.
- 2.2.** Listez les modifications à apporter pour disposer d'un système de traçabilité conforme aux recommandations d'usage.

Dossier documentaire**Document 1****Résultat du test n° 1**

Test n° 1 : Analyse du code source à l'aide d'un scanner de vulnérabilité

Vulnérabilité XSS trouvée : niveau de risque élevé

Description	Le <i>cross-site-scripting</i> (XSS) est un type de faille de sécurité des sites Web permettant d'injecter du contenu dans une page, provoquant ainsi l'exécution de code malveillant du type Javascript lors de chaque visite de la page infectée. Une attaque XSS peut modifier le contenu de la base de données et permettre à un attaquant de capturer des cookies d'identifiants de sessions et ainsi s'identifier sur les comptes des victimes sans connaître le mot de passe.
Détail de la vulnérabilité	URL Get input commentaire_commande was set to 1"()"%<cx><sCRIPt>vf8s(9896)</script> in page panier.php
Conseil pour la correction de la vulnérabilité	<ol style="list-style-type: none"> 1. Vérification des données saisies dans le champ commentaire_commande afin de repérer qu'il n'y a pas de caractères suspects associés à du code malveillant via une liste noire de caractères interdits. 2. Encodage des données saisies afin de rendre impossible l'exécution de code malveillant via la fonction htmlspecialchars : <code>string htmlspecialchars (string)</code>. La fonction htmlspecialchars convertit des caractères spéciaux en entités HTML rendant impossible l'exécution de code malveillant (SQLi, XSS). La fonction reçoit en paramètre la chaîne à convertir et renvoie comme résultat une chaîne encodée. Par exemple, la chaîne <code><script></code> devient <code>&lt;script&gt;</code>.

Document 2**Extrait du code source contenant la vulnérabilité**

```

1- <?php
2- //1-Récupération du commentaire saisi par l'utilisateur.
3- $commentaire = $_POST['commentaire_commande'];
4- //2-Exécution de la requête.
5- $requete = "UPDATE Commande set commentaire_commande = '$commentaire'
6-           where id_commande =$_SESSION[IdCommande];
7- mysqli_query($requete);

```

Document 3**Résultat du test n° 2**

Test n° 2 : Calcul de la somme de contrôle (hash) du fichier de configuration apache2.conf. Ce fichier permet de piloter toute la configuration du serveur Web qui héberge le site extranet (activation du chiffrement, modules chargés...).

- Somme de contrôle du fichier apache2.conf de configuration du serveur Web calculée avant l'attaque et conservée par Fermabio

Algorithme utilisé	SHA256
Fichier de configuration testé	/etc/apache2/apache2.conf
Somme de contrôle	bc6682a799eaf7056e9ba0ffe6d6fb5f5d57f9422f07cfb69f634b2ddcab767

- Somme de contrôle du fichier apache2.conf de configuration du serveur Web calculée lors de l'intervention de Securenet

Algorithme utilisé	SHA256
Fichier de configuration testé	/etc/apache2/apache2.conf
Somme de contrôle	bc6682a561eaf7056e9ba0ffe6d6fb5f5d57f9422f07cfb69f634b2ddpom767

Document 4

Configuration de la collecte des journaux systèmes de Fermabio

Le *cluster* de pare-feu PfSense est configuré pour enregistrer les journaux systèmes et présente les caractéristiques suivantes :

Date et heure affichée	Vendredi 29 novembre 2019, 08h05
Fuseau horaire	America/Denver
Méthode d'enregistrement	Temps différé : transfert des journaux sur les disques de conservation chaque fin de semaine
Centralisation des <i>logs</i>	Non
Méthode de transfert vers les disques	HTTP

Entraînement à l'épreuve E6

L'organisation cliente

DRONE-SÉCURITÉ est une entreprise spécialisée dans la fabrication de drones professionnels et la prise de vues aériennes. Implantée à Ambazac (proche de Limoges) et forte de 15 années d'expérience, DRONE-SÉCURITÉ propose diverses prestations de services comme le survol de sites industriels ou la formation au pilotage de drones.

La société est toujours à la pointe dans l'utilisation des nouvelles technologies et développe des applications pour répondre à ses propres besoins et à ceux de ses clients.

Aujourd'hui, DRONE-SÉCURITÉ compte une cinquantaine de salariés répartis sur cinq unités :

- un atelier de fabrication ;
- un service de recherche et développement ;
- un entrepôt pour les tests et la production de prototypes ;
- un service informatique ;
- un service de direction générale chargé de la gestion administrative et commerciale.

Une nouvelle activité a été lancée depuis quelques mois : l'utilisation de drones pour les exploitations agricoles. Les drones repèrent les dégâts de nuisibles sur les cultures et permettent d'optimiser l'exploitation des terres en captant de nombreuses données : niveau d'azote, de chlorophylle, biomasse, taux d'humidité, etc.

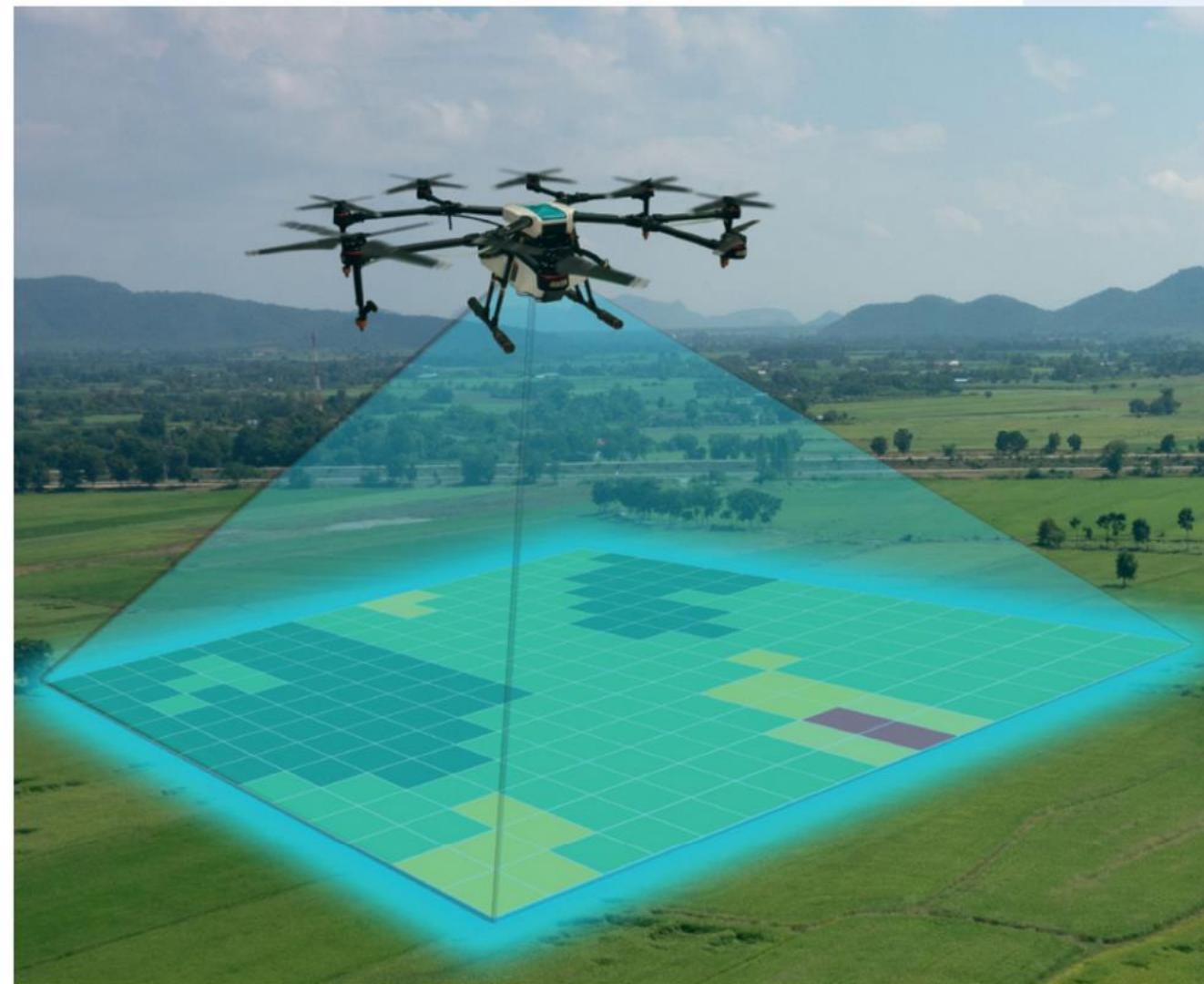
Une application nommée GéoMap est actuellement testée pour faciliter l'analyse des données collectées et aider l'exploitant à adapter précisément le niveau d'engrais ou d'autres produits phytosanitaires à appliquer sur ses parcelles.

Lorsqu'un agriculteur s'inscrit, il bénéficie d'un vol de reconnaissance de son exploitation réalisé par un pilote de DRONE-SÉCURITÉ. Le traitement des données collectées chez les exploitants agricoles est actuellement confié à l'entreprise VID&O. Elle fournit une synthèse de l'analyse des données à DRONE-SÉCURITÉ et au client.

Le développement de la nouvelle activité de drones pour les exploitations agricoles soulève quatre interrogations majeures :

- Les données à caractère personnel collectées et traitées pendant le vol de reconnaissance sont-elles sécurisées ?
- Comment protéger l'identité numérique de DRONE-SÉCURITÉ face à des tentatives d'hameçonnage visant à obtenir les données des exploitants agricoles ?
- Comment sécuriser l'usage des drones par les exploitants agricoles ?
- L'accès à l'application GéoMap par les exploitants agricoles est-il garanti face à des cyberattaques ?

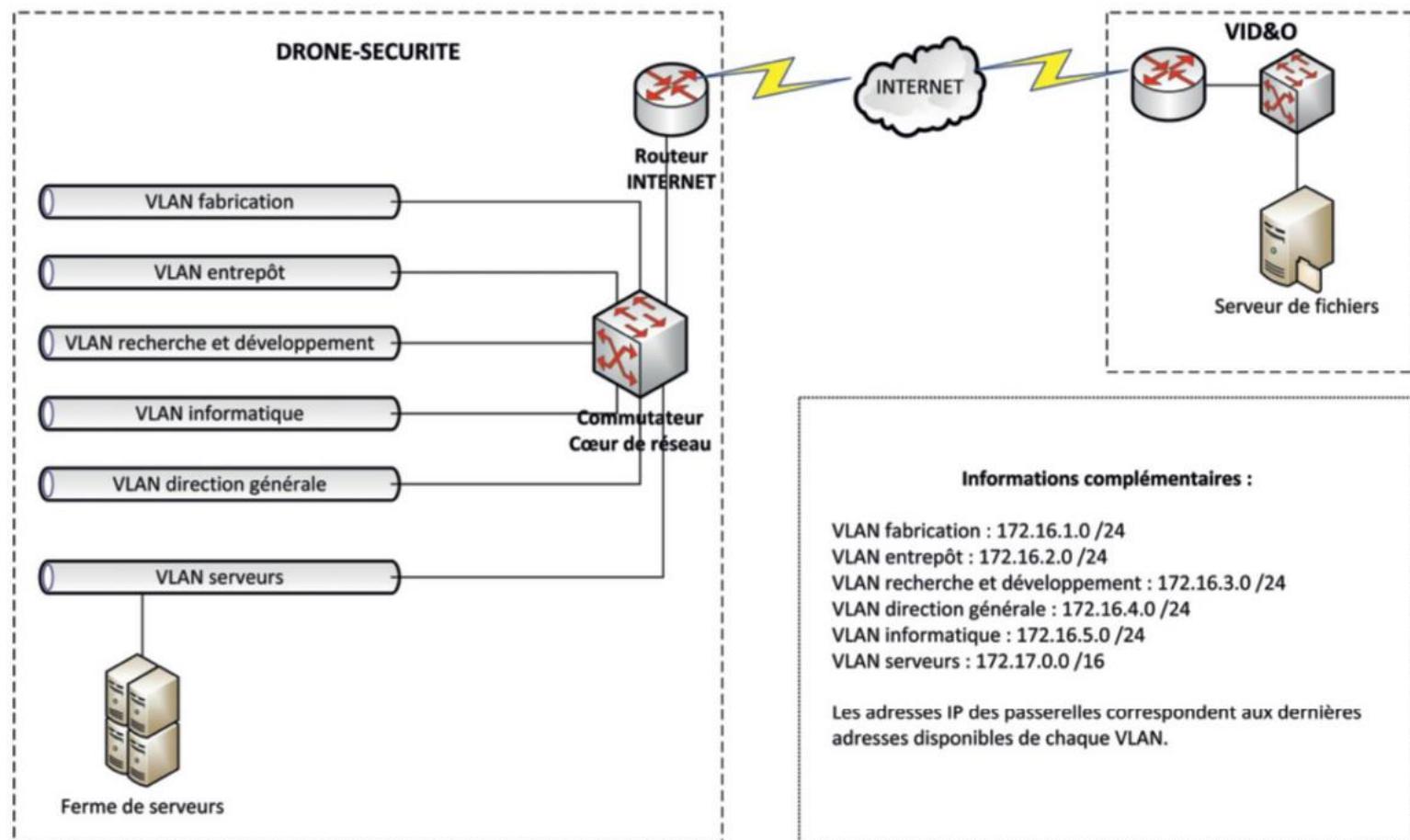
Le réseau informatique est géré par la direction des systèmes d'information (DSI) de la société. La DSI fait appel à un prestataire informatique pour réaliser un audit sur le respect de la législation et la sécurisation de son système d'information (SI) : SIO-INFO.



Le prestataire informatique

L'entreprise SIO-INFO, placée parmi les leaders de son domaine, est mandatée pour réaliser un audit concernant l'impact de la nouvelle activité de DRONE-SÉCURITÉ sur son SI. Vous intégrez cette entreprise et vous devez accompagner vos collègues dans les opérations d'audit liées aux quatre interrogations identifiées.

Architecture réseau de DRONE-SÉCURITÉ



Votre mission

Votre mission consiste à aider vos collègues dans le traitement des quatre dossiers d'audit.

Dossier A : La protection des données personnelles dans le cadre des vols de reconnaissance

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

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

Dossier D : La garantie de la disponibilité et de l'intégrité des services informatiques de DRONE-SÉCURITÉ et de leurs données face à une cyberattaque de l'application GéoMap

Vous vous appuyez sur le dossier documentaire mis à votre disposition.

A

Déployer les moyens appropriés de preuves électroniques

➤ Documents A.1 à A.6

Un vol de reconnaissance doit être réalisé pour tout nouvel exploitant par un pilote de DRONE-SÉCURITÉ afin d'étudier et d'analyser la parcelle agricole. Plusieurs données sont collectées (exemple : mesures du niveau d'azote), dont certaines à caractère personnel comme des images de la propriété privée de l'exploitant. De nombreux exploitants ont le statut d'entreprise individuelle, ce qui amène DRONE-SÉCURITÉ à être particulièrement vigilant sur la protection de leurs données personnelles.

Missions

1

Analyse des risques sur les traitements des données à caractère personnel

Suite à une perte récente de données acquises lors d'un vol de reconnaissance, M^{me} Carreter, responsable des traitements des données chez DRONE-SÉCURITÉ, vous demande d'analyser les scénarios de menaces envisageables et de proposer des solutions correctrices.

- 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.
- 1.2.** Analysez la vraisemblance de chaque scénario et la gravité des risques sur les traitements des données à caractère personnel.
- 1.3.** Proposez une solution technique pour chaque scénario de menaces permettant de renforcer la protection des données à caractère personnel.

2

Vérification de la conformité avec la législation du traitement des données personnelles

Un récent courriel envoyé par le voisin d'un exploitant agricole a alerté DRONE-SÉCURITÉ sur la captation d'images de sa propriété privée et leur mise en ligne sur le site vitrine de l'exploitant. La DSI de DRONE-SÉCURITÉ vous communique les premiers éléments de diagnostic ainsi qu'un extrait du contrat de sous-traitance pour identifier sa vulnérabilité et apporter des éléments de réponse.

Vous devez identifier les responsabilités de chaque acteur et apporter une réponse technique à l'incident.

- 2.1.** Retrouvez, parmi les engagements du sous-traitant, ceux qui peuvent contribuer à renforcer la protection des données à caractère personnel.
- 2.2.** Identifiez l'acteur responsable de la publication d'images privées sur le site de l'exploitant.
- 2.3.** Proposez une solution technique permettant une mise en conformité de la protection des données à caractère personnel.

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

› Documents B.1 à B.8

M^{me} Dejean, du service de direction générale, vous contacte suite à l'appel d'un exploitant agricole qui vient de recevoir un courriel lui proposant de souscrire un contrat d'assurance sur le matériel informatique. Cet exploitant est mécontent car il pensait n'avoir rien d'autre à payer, en plus du contrat initialement souscrit.

Or, ce type de contrat d'extension de garantie n'est pas proposé par la société DRONE-SÉCURITÉ. M^{me} Dejean s'inquiète des répercussions possibles de cette tentative d'hameçonnage (*phishing*) utilisant le nom de DRONE-SÉCURITÉ.

Missions

1 Protection de l'identité numérique de l'organisation suite à une attaque par usurpation d'identité

M^{me} Dejean vous demande d'analyser la tentative d'hameçonnage et de proposer des solutions correctrices.

- 1.1. Repérez les éléments, dans le courriel reçu par l'exploitant agricole, permettant de reconnaître une opération d'hameçonnage.
- 1.2. Identifiez les risques pour DRONE-SÉCURITÉ de la multiplication des avis négatifs publiés sur les réseaux sociaux en rapport à cette cyberattaque.
- 1.3. Proposez une solution technique qui permettrait de sécuriser les échanges entre la société et ses clients.

2 Déploiement de moyens appropriés de preuves électroniques liées à l'usurpation d'identité

La société DRONE-SÉCURITÉ doit faire face à des conséquences inattendues de cette attaque par typosquattage de l'URL. En effet, cette attaque utilisant un nom de domaine assez proche du site officiel a pour conséquence de détourner une partie des données du site de la société DRONE-SÉCURITÉ.

- 2.1. Repérez les éléments dans l'URL du lien communiqué qui permettent d'identifier une attaque par typosquattage.
- 2.2. Identifiez les risques juridiques encourus pour DRONE-SÉCURITÉ par le typosquattage de son site et le recueil de données personnelles de ses clients.
- 2.3. Rédigez une note avec vos recommandations sur les moyens de défense face à une attaque de ce type.

La sécurisation de l'usage des drones par les exploitants

› Documents C.1 à C.6

Afin de faciliter les échanges entre les exploitants agricoles, le service informatique de DRONE-SÉCURITÉ a créé un espace sécurisé (extranet) sur son site. L'objectif est de créer une communauté autour de l'utilisation des drones pour y recevoir des conseils ou des témoignages.

Ce service doit permettre une authentification sécurisée afin de protéger les informations de chacun. De plus, DRONE-SÉCURITÉ désire créer une connexion directe des utilisateurs à un espace de stockage dédié depuis un navigateur Internet afin qu'ils puissent télécharger les données prélevées sur leurs exploitations (vidéos et images).

SIO-INFO est chargé de proposer des procédures et des outils permettant d'assurer la sécurité de ces différents services.

Missions

1

Création des éléments d'authentification

SIO-INFO propose une procédure et un dispositif permettant la création des identifiants de connexion et une authentification avec un haut niveau de sécurité.

L'utilisation des drones est, comme toute utilisation d'objets connectés, soumise à des risques de cyberattaques. C'est pourquoi SIO-INFO a décidé de mener une étude pour identifier les plus récurrentes afin d'apporter des solutions appropriées pour limiter les risques.

- 1.1.** Expliquez pourquoi le formulaire de création des identifiants de connexion permet une authentification sécurisée.
- 1.2.** Précisez l'objectif de la procédure d'authentification décrite. Justifiez votre réponse en spécifiant le type d'authentification utilisée.
- 1.3.** Indiquez si la procédure d'initialisation des drones chez DRONE-SÉCURITÉ permet d'éviter les failles de sécurité décrites dans l'étude.

2

Gestion des accès aux données

Les données récoltées par les drones sont stockées sur le serveur de fichiers dans un dossier de partage. Grâce à une connexion sécurisée (VPN, Virtuel Private Network), les utilisateurs ont accès au VLAN du serveur de fichiers et peuvent ainsi consulter ou télécharger l'ensemble de leurs données personnelles.

SIO-INFO est chargé de proposer une configuration et une architecture réseau permettant de contrôler les habilitations et les accès de chaque utilisateur.

- 2.1.** Montrez comment la configuration des partages permet de contrôler l'accès aux données.
- 2.2.** Précisez l'intérêt de séparer (dans un autre VLAN) le serveur de fichiers des autres serveurs.

La garantie de la disponibilité et de l'intégrité des services informatiques et des données de DRONE-SÉCURITÉ face à une cyberattaque de l'application GéoMap

› Documents D.1 à D.7

La nouvelle application GéoMap de DRONE-SÉCURITÉ permet la mise en place d'une stratégie d'agriculture raisonnée. Après avoir effectué une analyse des besoins, le service de recherche et développement a livré une première version de cette application à quelques exploitants pour la réalisation de tests. SIO-INFO est chargé d'auditer la sécurité de cette nouvelle application.

Missions

1

Sécurisation de la page d'authentification de l'application GéoMap

Dans cette première mission, SIO-INFO audite la sécurité de la page d'authentification de GéoMap. Afin de la sécuriser, SIO-INFO propose le développement de deux méthodes supplémentaires dans la classe InputAuthenticationHelper.

- 1.1. Précisez pourquoi le développement de la page d'authentification de GéoMap doit faire l'objet de toutes les attentions.
- 1.2. Expliquez en quoi la première version du code source de la page d'authentification de GéoMap n'est pas sécurisée.
- 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.
› Le code source à compléter figure dans le document D.4 : ajoutez uniquement la partie de code nécessaire en indiquant les numéros des lignes concernées.

2

Gestion des traces de tentatives d'authentification sur GéoMap

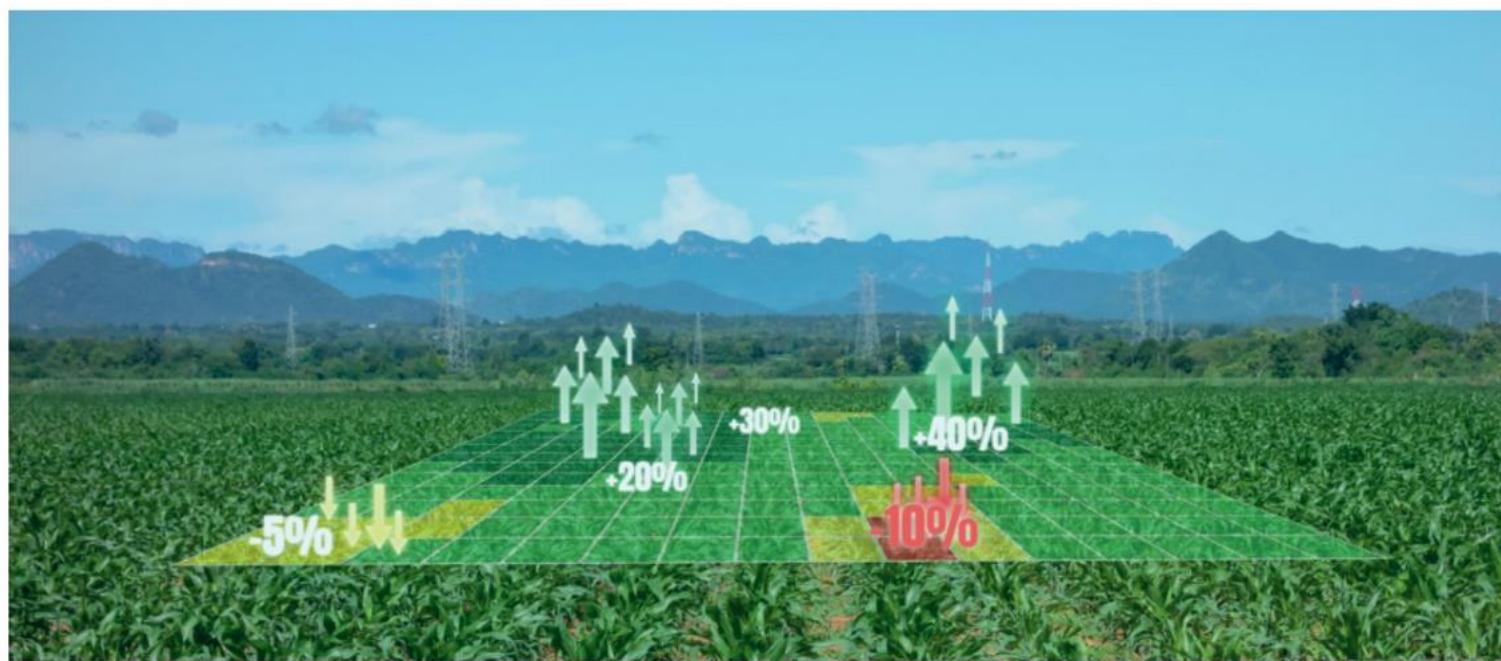
SIO-INFO a terminé son travail d'audit en définissant une politique permettant de tracer les tentatives d'authentification sur l'application GéoMap. Votre mission consiste à adapter l'application GéoMap à cette recommandation de sécurité.

- 2.1. Quel peut être l'intérêt de tracer les tentatives d'authentification ?
- 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.
› Le code source à compléter figure dans le document D.4 : ajoutez uniquement la partie de code nécessaire en indiquant les numéros des lignes concernées.

Dossier documentaire A

Document 1

Organisation du vol de reconnaissance



• **M. Durand (salarié de SIO-INFO)** : Bonjour, madame Carreter, je suis monsieur Durand, salarié de la société SIO-INFO, mandatée par votre direction pour la réalisation d'un audit de votre nouvelle activité concernant l'utilisation de drones pour les exploitations agricoles.

Je m'intéresse, dans un premier dossier, à l'organisation du vol de reconnaissance rendu obligatoire pour toute nouvelle inscription. Pouvez-vous m'en résumer les principales étapes ?

• **M^{me} Carreter (responsable des traitements chez DRONE-SÉCURITÉ)** : Bonjour monsieur Durand, un nouvel exploitant doit s'inscrire au préalable sur notre site internet en indiquant ses coordonnées personnelles et quelques informations sur son exploitation (taille de la parcelle, statut juridique...). Ensuite, il doit choisir une date d'intervention parmi celles proposées pour l'organisation d'un vol de reconnaissance.

• **M. Durand** : Pouvez-vous m'expliquer l'organisation de ce vol de reconnaissance ?

• **M^{me} Carreter** : Le vol de reconnaissance est très important pour nous puisqu'il doit permettre d'aboutir à un contrat commercial.

Le jour de l'intervention, un pilote de DRONE-SÉCURITÉ vient chez l'exploitant avec un drone pour réaliser

un survol d'une heure de la parcelle qui permet de collecter les premières données sur l'exploitation agricole et un enregistrement vidéo.

L'ensemble de ses données est enregistré dans une carte SSD positionnée sur le drone.

• **M. Durand** : Quel est le rôle du pilote dans ce processus ?

• **M^{me} Carreter** : Le pilote doit réaliser les premiers paramétrages du drone et, à la fin du vol de reconnaissance, il doit ramener la carte SSD, contenant les données collectées pendant le vol dans les locaux de DRONE-SÉCURITÉ.

Ces données sont stockées dans un dossier se situant sur son poste de travail. Ensuite il doit se connecter via un identifiant et un mot de passe unique pour tous les pilotes au serveur FTP depuis son poste de travail pour transférer les données vers un espace de stockage hébergé chez un sous-traitant : VID&O.

• **M. Durand** : Pouvez-vous me préciser le rôle du sous-traitant VID&O ?

• **M^{me} Carreter** : VID&O doit traiter les données et rédiger un rapport sur la qualité du sol de la parcelle à destination de l'exploitant et de DRONE-SÉCURITÉ. Il détient des données d'identification (coordonnées de l'exploitant, données de géolocalisation ou encore des enregistrements vidéo du vol).

Document 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	...
Scénario 3	...

Document 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 l'ensemble des données contenues dans la carte)	
Scénario 2			
Scénario 3			

C : Confidentialité ; D : Disponibilité ; I : Intégrité.

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

Document 4

Niveau de gravité d'un risque

Scénario 1	Perte de la carte SSD	Niveau de gravité : 3 Les données confidentielles peuvent être utilisées par une personne non habilitée.
Scénario 2	...	
Scénario 3	...	

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

Document 5

Diagnostic technique du serveur FTP

- Écoute du transfert FTP réalisée par le pilote vers l'espace partagé

No	Time	Source	Destination	Protocol	Info
33	12.294108	158.91.170.5	172.16.5.10	FTP	Response : 220-FileZilla Server version 0.9.41 beta
34	12.294398	158.91.170.5	172.16.5.10	FTP	Response : 220-written by Tim Kosse
35	12.294456	158.91.170.5	172.16.5.10	FTP	Response : 220 Please visit http://sourceforge.net
37	12.297950	172.16.5.10	158.91.170.5	FTP	Request : AUTH TLS
38	12.298919	158.91.170.5	172.16.5.10	FTP	Response : 520 SSL/TLS authentication not allowed
39	12.301404	172.16.5.10	158.91.170.5	FTP	Request : AUTH TLS
40	12.301927	158.91.170.5	172.16.5.10	FTP	Response : 520 SSL/TLS authentication not allowed
49	17.203661	172.16.5.10	158.91.170.5	FTP	Response : USER pilote
50	17.204192	158.91.170.5	172.16.5.10	FTP	Response : 331 Password required for pilote
51	17.206974	172.16.5.10	158.91.170.5	FTP	Response : PASS drone
52	17.207480	158.91.170.5	172.16.5.10	FTP	Response : 223 Logged on

• • •

- Écoute du transfert FTP réalisée par VID&O vers l'espace partagé

No	Time	Source	Destination	Protocol	Info
33	25.294108	158.91.170.5	192.168.0.10	FTP	Response : 220-FileZilla Server version 0.9.41 beta
34	25.294398	158.91.170.5	192.168.0.10	FTP	Response : 220-written by Tim Kosse
35	25.294456	158.91.170.5	192.168.0.10	FTP	Response : 220 Please visit http://sourceforge.net
37	25.297950	192.168.0.10	158.91.170.5	FTP	Request : AUTH TLS
38	25.298919	158.91.170.5	192.168.0.10	FTP	Response : 234 Using authentication type TLS
39	25.301404	192.168.0.10	158.91.170.5	FTP	Request : \026\003\005\002
40	25.301927	158.91.170.5	192.168.0.10	FTP	Response : \002\023\004

Document 6

Extrait du contrat de sous-traitance

- Article 1 - Garanties suffisantes

Le sous-traitant certifie disposer des compétences techniques (IT, sécurité, infrastructure...) et juridiques pour appréhender l'ensemble des obligations qui sont imposées par le règlement pour le traitement des données personnelles qui lui seront transmises par le responsable du traitement. Il certifie également avoir les ressources suffisantes pour garantir en permanence son respect. À ces fins, le sous-traitant transmet l'ensemble des éléments probatoires nécessaires à cette démonstration.

- Article 2 - Obligation juridique, objet et durée du traitement

Ce contrat lie juridiquement le sous-traitant au responsable de traitement dans la fourniture de prestations de service opérant le traitement de données personnelles pour son compte.

L'objet du contrat est le traitement de vidéos et de données concernant le survol en drones d'exploitations agricoles.

La durée du traitement prévue au contrat est définie par l'abonnement annuel pris par le responsable du traitement jusqu'à notification d'arrêt des services.

- Article 3 - Nature et finalité du traitement

Le traitement de données personnelles par sous-traitant vise à réaliser une synthèse sur l'étude des données collectées lors du survol de drones et le traitement des images à destination de DRONE-SÉCURITÉ.

- Article 4 - Type de données traitées

Les données personnelles traitées sont :

- les captations vidéo de l'exploitation agricole ;
- les images collectées ;
- les coordonnées personnelles de l'exploitant agricole (nom, prénom, adresse, numéro de téléphone, e-mail).

- Article 5 - Les engagements sur les données personnelles

Engagement n° 1 : la non réutilisation des données hébergées sur nos services

Les informations hébergées dans le cadre de nos services restent la propriété du client. Nous nous interdisons toute revente desdites données, de même que toute utilisation à des fins commerciales (telles des activités de profilage ou de marketing direct).

Engagement n° 2 : permettre la réversibilité de vos données

Chez VID&O, 100 % de nos solutions de *cloud* sont basées sur des standards, dont un certain nombre de technologies open source. Vous pouvez donc récupérer vos données facilement : la réversibilité et l'interopérabilité sont toujours possibles.

Engagement n° 3 : vous informer en cas de violation de données

Dans l'éventualité d'une violation d'informations, nous nous engageons à informer les clients concernés dans les meilleurs délais. Cette notification précise la nature de l'incident, ses conséquences prévisibles, ainsi que les mesures prises pour résoudre ou minimiser la violation.

Dossier documentaire B

Document 1

Copie du courriel reçu par M^{me} Dejean de l'exploitant agricole pour pouvoir vérifier la véracité de l'offre

Cher(e) client(e)

Merci de lire attentivement ce courriel. Il contient des informations essentielles, destinées à faciliter l'utilisation de votre compte chez DRONE-SÉCURITÉ et le recours à ses différents services.

DRONE-SÉCURITÉ à l'honneur de vous annoncer qu'elle a enfin mis à votre disposition un service d'assurance et d'assistance sur l'ensemble de vos matériels informatique.

Pour en savoir plus et accéder au formulaire d'inscription à ce programme. Veuillez cliquer sur le lien ci-dessous :

<http://www.drones-securite.fr>

Pour plus d'informations, nous vous invitons à consulter l'un des supports proposés ci-dessous : Par e-mail : drones-securite@services-clients.fr, n'oubliez pas de vous munir de votre identifiant, mot de passe et numéro client pour faciliter le traitement de votre dossier.

Hotline : 32 44 (0,34 euro/min depuis une ligne fixe). Le service est disponible 24h/24h, 7jours/7.

Merci de la confiance que vous nous témoignez.
L'équipe commercial de DRONE-SÉCURITÉ

Document 2

Extrait d'échanges sur Twitter entre exploitants en colère

JeunePaysanCreuze23
@JPC23



Suivre

@DroneSécurité abusé votre assurance pour du matériel que j'ai payé perso. C'est quoi cette arnaque ?

#DroneSécuritéAssurance

12 :23 – 12 Mars 2020

247

884

492



LEGOFERMIER
@legOFermier



Suivre

@DroneSécurité et en plus il faut payer la hotline pour comprendre

#DroneSécuritéAssurance

12 :31 – 12 Mars 2020

252

188

214

Document 3

Comment repérer une arnaque reçue dans votre messagerie ou votre boîte mail ?

Soyez attentif au niveau de langage du courriel : même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration...).

Vérifiez les liens dans le courriel : avant de cliquer sur les éventuels liens, laissez votre souris dessus. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Ne

faites pas confiance aux noms de domaine du type impots.gouv.fr, impots.gouvfr.biz, infocaf.org au lieu de www.caf.fr.

Méfiez-vous des demandes étranges : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code de carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.

Source : CNIL

Document 4

Extrait des recommandations pour assurer l'intégrité, la confidentialité et l'authenticité d'une information

Les fonctions de hachage permettent d'assurer l'intégrité des données. Les signatures numériques, en plus d'assurer l'intégrité, permettent de vérifier l'origine de l'information et son authenticité. Enfin, le chiffrement, parfois improprement appelé cryptage, permet de garantir la confidentialité d'un message.

Les précautions élémentaires :

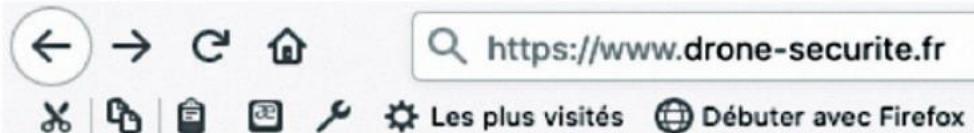
- utiliser un algorithme reconnu et sûr ;
- utiliser les tailles de clés suffisantes ;
- protéger les clés secrètes, au minimum par la mise en œuvre de droits d'accès restrictifs et d'un mot de passe sûr ;
- rédiger une procédure indiquant la manière dont les clés et certificats vont être gérés en prenant en compte les cas d'oubli de mot de passe de déverrouillage.

Source : CNIL

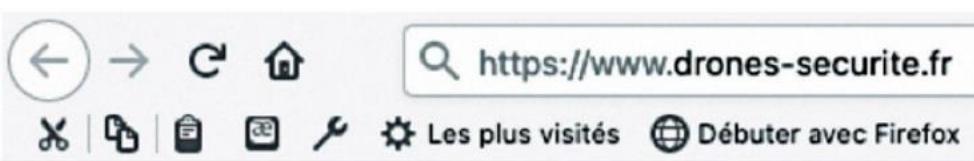
Document 5

Vérification d'URL

• Site Officiel de DRONE-SÉCURITÉ



• Faux site

**Échec de la connexion sécurisée**

Une erreur est survenue pendant une connexion à 10000-sans.badssl.com. SSL a reçu un enregistrement « Handshake » malformé. Code d'erreur : SSL_ERROR_RX_MALFORMED_HANDSHAKE

- La page que vous essayez de consulter ne peut pas être affichée car l'authenticité des données reçues ne peut être vérifiée.
- Veuillez contacter les propriétaires du site web pour les informer de ce problème.

[En savoir plus...](#)

Document 6**Extrait du rapport sur l'état de la menace liée au numérique**

Le typosquatting est une technique consistant à acheter des noms de domaine qui ressemblent étrangement à des noms de site connus, mais avec des fautes volontaires, comme des erreurs orthographiques. Quatre principaux types de typosquattage d'une URL sont identifiés :

- utilisation d'un même terme mais écrit différemment ;
- une faute orthographique ou une homonymie ;
- un autre domaine de premier niveau (top-level domain ou TLD) comme .org au lieu de .com ;
- ou encore en utilisant les fautes de frappe de l'internaute.

Ces achats peuvent être considérés comme des actes préparatoires à des attaques de type *spear-phishing* (campagne de faux courriels ciblés). Le typosquatting

permet de mettre en confiance les destinataires et ainsi de les tromper.

Ainsi, début 2018, une campagne de *phishing* particulièrement évoluée, promettant des billets de vol gratuits, a pu sévir en employant une technique de l'homoglyphe de nom de domaine, difficile à déceler car la lettre « a » est remplacée par le caractère « à » avec rond souscrit. L'URL utilisée renvoie, comme toujours, sur un site de *phishing* contrôlé par les pirates, demandant aux victimes de rentrer leurs coordonnées bancaires pour valider cette opération. Ce type d'attaque est possible, car il est, en effet, possible d'enregistrer des noms de domaines avec des caractères d'alphabets non latins.

Source : *Rapport n° 2, mai 2018 – Ministère de l'intérieur*

Document 7**La voie extrajudiciaire avec la procédure UDRP
(uniform domain name dispute resolution policy)**

Cette procédure, rapide, entièrement en ligne et ne nécessitant pas un avocat, a été mise en place par l'ICANN* pour régler les problèmes liés au typosquatting. Elle peut être engagée sans préjudice d'une action devant les instances judiciaires compétentes.

Cette procédure ne concerne que les noms dont l'extension est .com, .net, .org, mais aussi les nouvelles telles que .biz, .info, .name.

Le plaignant doit prouver que le registrant du nom de domaine pirate a enregistré ou fait un usage de mauvaise foi du nom de domaine sur lequel le plaignant a des droits et pour lequel le défendeur n'a aucun intérêt légitime.

Pour les litiges concernant les extensions en .fr et .re, la procédure est nommée PARL et suit le même modèle que la procédure UDRP.

* ICANN : Internet Corporation for Assigned Names and Numbers est une autorité de régulation d'Internet.

Document 8**Article L. 45-2 du Code des postes et des communications**

Dans le respect des principes rappelés à l'article L. 45-1, l'enregistrement ou le renouvellement des noms de domaine peut être refusé ou le nom de domaine supprimé lorsque le nom de domaine est :

1° susceptible de porter atteinte à l'ordre public ou aux bonnes mœurs ou à des droits garantis par la Constitution ou par la loi ;

2° susceptible de porter atteinte à des droits de propriété intellectuelle ou de la personnalité, sauf si le demandeur justifie d'un intérêt légitime et agit de bonne foi ;

3° identique ou apparenté à celui de la République française [...].

Peut notamment caractériser l'existence d'un intérêt légitime, pour l'application du 2° et du 3° de l'article L. 45-2, le fait, pour le demandeur ou le titulaire d'un nom de domaine :

- d'utiliser ce nom de domaine, ou un nom identique ou apparenté, dans le cadre d'une offre de biens ou de services, ou de pouvoir démontrer qu'il s'y est préparé ; [...]
- d'avoir obtenu ou demandé l'enregistrement d'un nom de domaine principalement dans le but de nuire à la réputation du titulaire d'un intérêt légitime ou d'un droit reconnu sur ce nom ou sur un nom apparenté, ou à celle d'un produit ou service assimilé à ce nom dans l'esprit du consommateur [...].

Dossier documentaire C

Document 1

Formulaire de création des éléments d'authentification

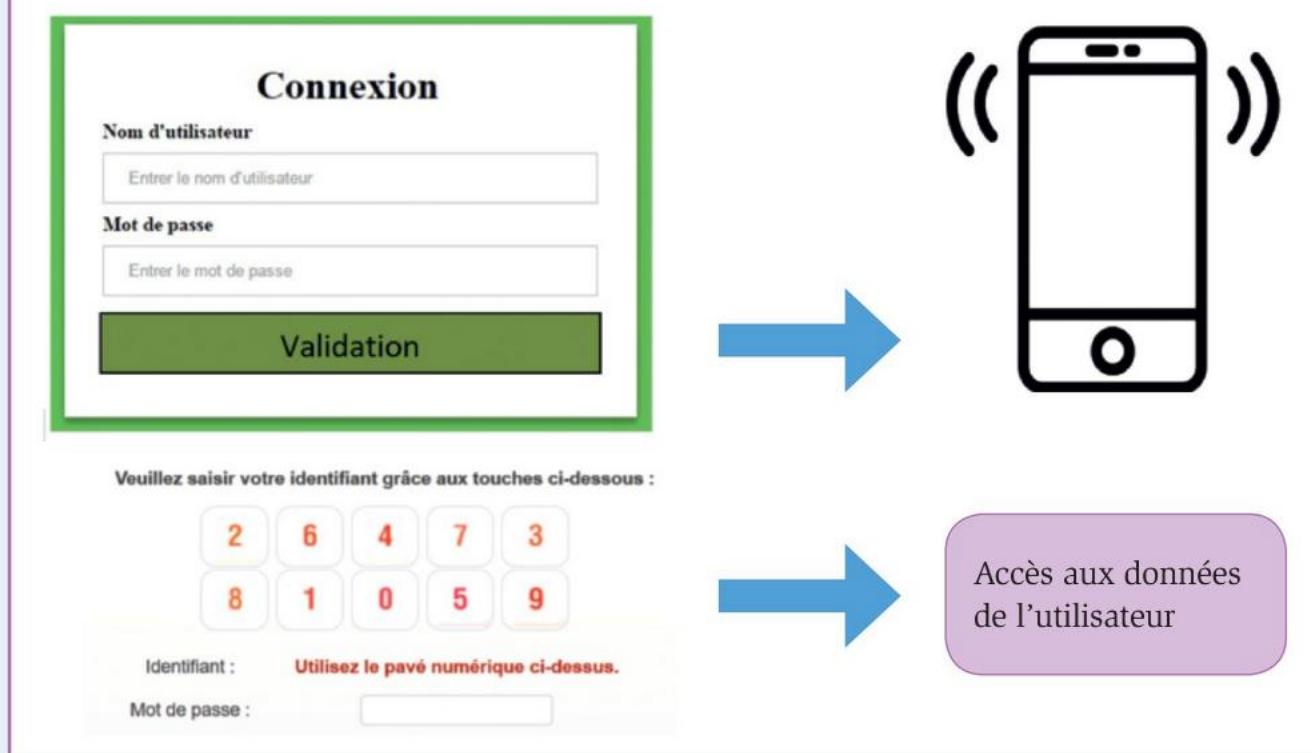
Extrait du code source de la page de création des éléments d'authentification : ici le code s'applique à la variable **password** qui contient le mot de passe créé par l'utilisateur.

```
<?php
$password = $_POST['password']; //récupère le mot de passe saisi dans le formulaire
if (preg_match('#^(?=.*[a-z])(?=.*[A-Z])(?=.*[0-9])(?=.*\W).{8,}$#', $password)) {
    //définit les différentes contraintes imposées lors de la création du mot de passe,
    //par exemple ( ?=.*\W) impose l'utilisation d'un caractère spécial
    echo 'Mot de passe conforme';
}
else {
    echo 'Mot de passe non conforme';
}
?>
```

```
<?php
$handle = fopen('dictionnaire.txt', 'r'); // On ouvre le dictionnaire en lecture seule
$buffer = «»; // Variable qui enregistre les mots extraits du fichier
$chaine = $_POST['password']; // On récupère le mot de passe de l'utilisateur
if ($handle)
{
    // Tant que l'on n'est pas à la fin du fichier on continue de parcourir les différents
    // Mots de passe et on les compare avec celui proposé par l'utilisateur.
    while (!feof($handle) AND ($buffer != $chaine))
    {
        $buffer = fgets($handle);
    }
    if ($buffer == $chaine) {
        // Le mot de passe est dans le fichier, il faut le changer !
    }
}
fclose($handle); // On ferme le fichier
?>
```

Document 2

Synthèse de l'étude sur les failles de sécurité



Document 3

Diagnostic sur l'authentification sur l'extranet des IoT

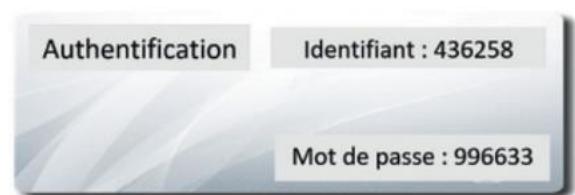
L'Internet des objets, ou IdO (en anglais, the *Internet Of Things*, ou IoT) peut se définir comme suit : « des objets qui captent, stockent, traitent et transmettent des données, qui peuvent recevoir et donner des instructions et qui ont, pour cela, la capacité de se connecter à un réseau d'information. Un fonctionnement articulé entre un objet, son capteur et une plateforme permet une analyse de données produites en quantité importante, en temps réel et personnalisée. » L'utilisation de ces objets se démocratise et nous les retrouvons aujourd'hui dans la plupart des foyers. Mais la cybersécurité des appareils ne s'améliore pas au fil du temps. Bien au contraire, le nombre de failles de sécurité a doublé au cours de ces six dernières années. De nombreux exemples d'attaques (drone DJI, Botnet Mirai, Botnet Brickerbot, Malware W32. Ramnit, etc.) nous ont permis d'identifier les deux principales failles de sécurité :

- Les éléments d'authentification et d'appareillage : les IoT utilisent en général des identifiants pré-configurés en mode usine simples et courants. Les fabricants n'imposent pas de les modifier lors du démarrage initial de l'appareil. Or, pour des raisons de coûts, de nombreux fabricants utilisent les mêmes données de connexion standards pour tous leurs appareils, au lieu de définir un mot de passe distinct pour chacun. De plus, les utilisateurs ne changent pas toujours le nom d'utilisateur ni le mot de passe existants par défaut.
- Le noyau Linux : de nombreux IoT exécutent des noyaux Linux obsolètes qui incluent des vulnérabilités et des failles critiques. Ici encore, pour limiter les coûts de fabrication, les entreprises n'incluent pas un espace de stockage suffisant sur leurs appareils pour permettre les mises à jour du noyau.

Document 4

Procédure d'initialisation des drones de DRONE-SÉCURITÉ par l'exploitant

Lors du premier démarrage du drone, initialisez les éléments d'authentification en indiquant l'identifiant et le mot de passe fournis par DRONE-SÉCURITÉ (carte authentification attachée au drone avec les deux séries de chiffres). Ces éléments d'authentification peuvent ensuite être modifiés par ceux de votre choix.

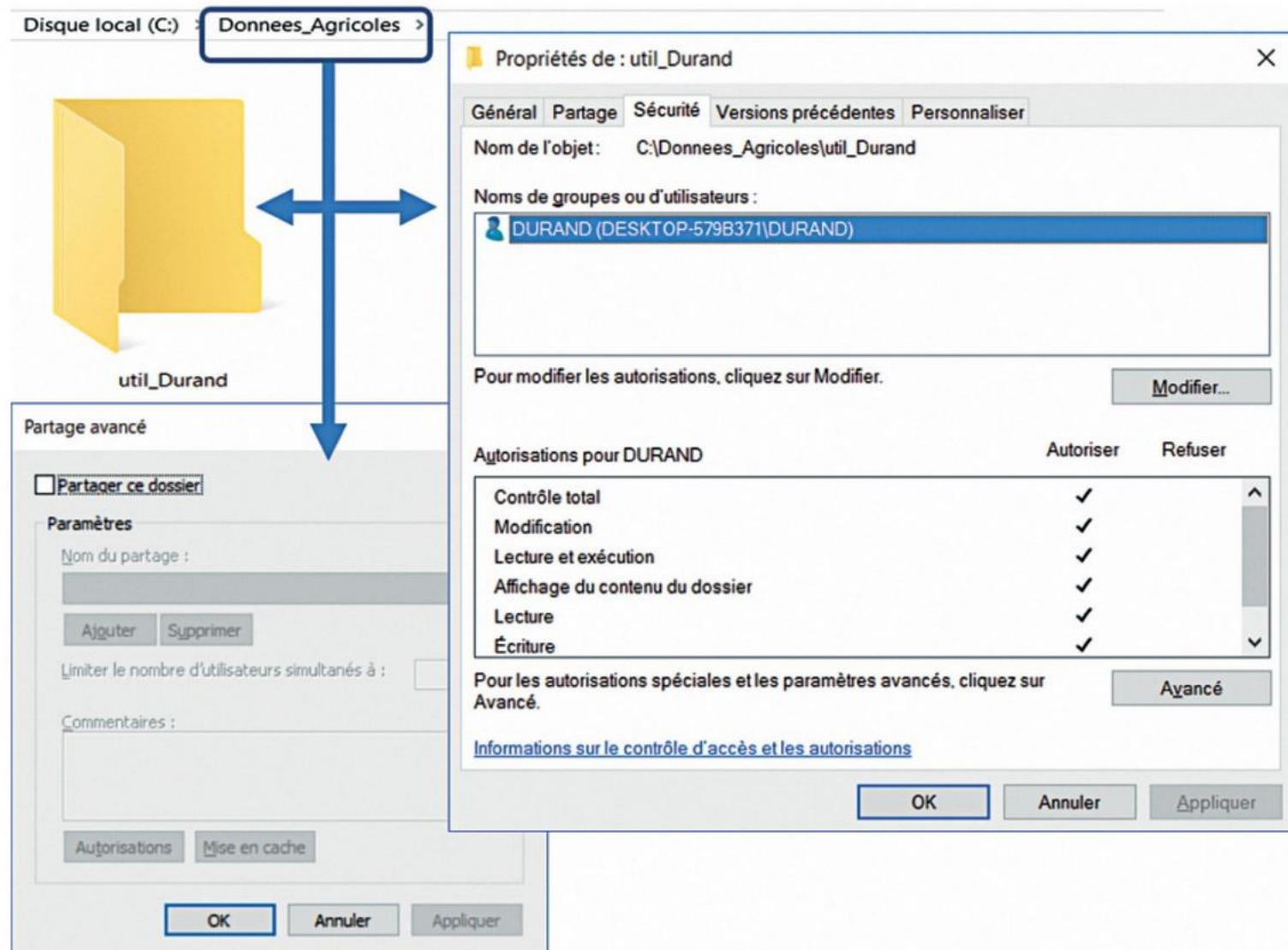


Après l'initialisation du drone, vous pouvez l'appareiller avec un smartphone ou une tablette via le WIFI ou le Bluetooth :

- * SSID Wifi : @DroneSecurite
- * Bluetooth : appareillage automatique

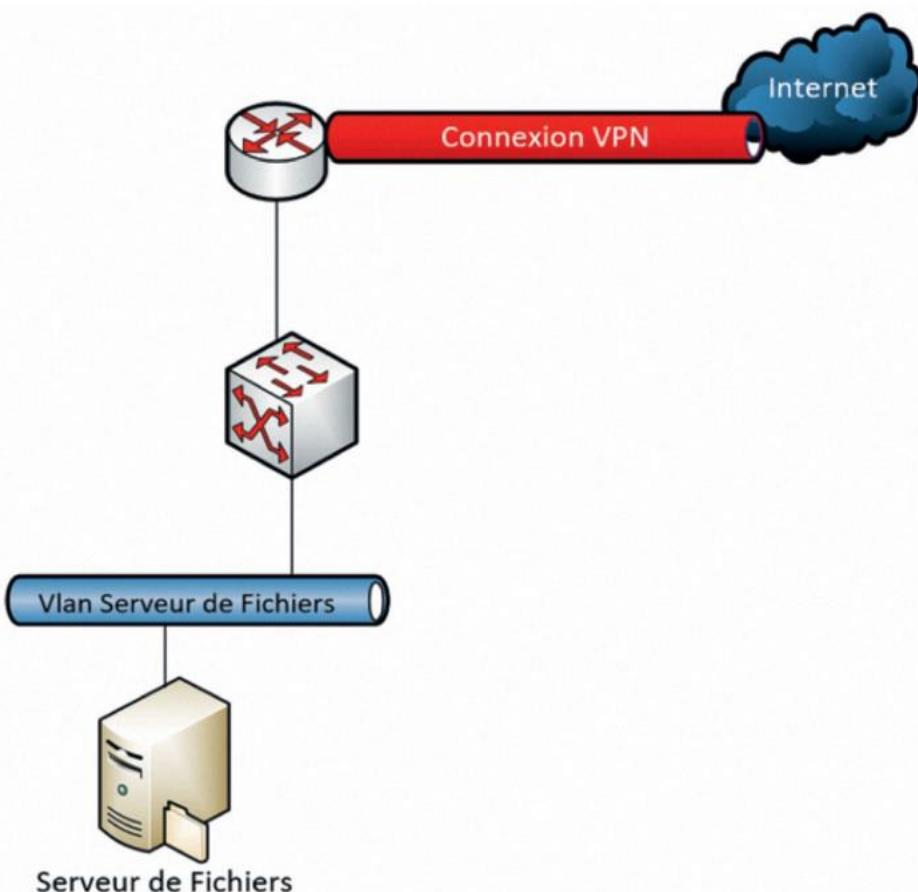
Document 5

Configuration des partages



Document 6

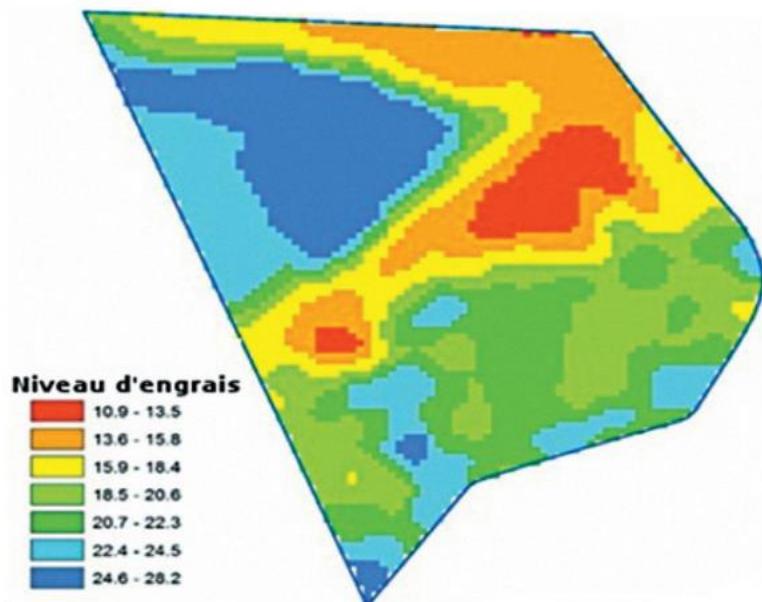
Nouvelle architecture réseau de DRONE-SÉCURITÉ



Dossier documentaire D

Document 1

Analyse des besoins de la nouvelle application Web GéoMap



SIO-INFO : Quels sont vos besoins concernant la nouvelle application GéoMap ?

DRONE-SÉCURITÉ : L'application GéoMap doit exploiter les données collectées par les drones et produire des cartes de terrains précises. Ces cartes permettent à l'agriculteur d'optimiser ses investissements. Les quantités d'engrais et de produits phytosanitaires à pulvériser sont indiquées en temps réel via un système de géolocalisation lors du déplacement de l'agriculteur sur ses parcelles.

SIO-INFO : L'application est donc constamment connectée à internet ?

DRONE-SÉCURITÉ : Oui, car les agriculteurs l'utilisent depuis leurs smartphones ou leurs tablettes *via* le réseau 4G. L'application suit l'agriculteur

au fur et à mesure de son déplacement et lui indique en temps réel le niveau d'arrosage et d'engrais à appliquer en fonction des zones parcourues.

SIO-INFO : Et concernant la sécurisation des accès ?

DRONE-SÉCURITÉ : Chaque agriculteur accède aux cartes de ses parcelles via la fourniture d'un identifiant et d'un mot de passe sur une page d'authentification accessible via le web. L'application est hébergée sur nos serveurs et développée sur AndroidStudio. Nous vous demandons d'étudier la sécurisation de la page d'authentification afin de garantir que seuls les agriculteurs ayant un compte légitime puissent accéder à leurs cartes.

Document 2

Extrait du code source de la première version de la page d'authentification de GéoMap

```

1 public class InputAuthenticationHelper {
2     public boolean checkAuth(String loginSaisi, String passwordSaisi)
3     {
4         boolean SuccessAuthentification = false;
5         Cursor cursor = db.rawQuery("select * from AGRICULTEURS where
6             USERNAME = '" + loginSaisi + "' and PASSWORD = '" + passwordSaisi + "';", null);
7         if (cursor != null) {
8             if (cursor.moveToFirst()) SuccessAuthentification = true;
9             cursor.close(); }
10        return SuccessAuthentification;
11    }
12 }
13 //loginSaisi et passwordSaisi contiennent les identifiants directement saisis depuis la
14 //page d'authentification de GEOMAP.
15 InputAuthenticationHelper oneAuth = new InputAuthenticationHelper();
16 if (oneAuth .checkAuth(loginSaisi,passwordSaisi) {
17     //Succès d'authentification, accès au compte privé de l'utilisateur...
18 }
```

Document 3

Extrait du code source de la première version de la page d'authentification de GéoMap

Les méthodes développées par SIO-INFO sont indiquées en gras.

```

1  public class InputAuthenticationHelper {
2      public boolean isValidInput(String input_utilisateur) {
3          // Vérifie qu'un champ saisi contient seulement les caractères autorisés
4          // (liste blanche) afin de prévenir les risques d'injection SQL
5          final String AUTH_PATTERN = "^[A-Za-z0-9-\\ ]+([\\.[A-Za-z0-9-]+([\\.[A-Za-z]{2,})$"
6          Pattern pattern = Pattern.compile(AUTH_PATTERN);
7          Matcher matcher = pattern.matcher(input_utilisateur);
8          return matcher.matches();
9      }
10     public boolean isValidLength(String input_utilisateur) {
11         // Vérifie le nombre de caractères afin de prévenir la saisie de code malveillant
12         Length_ok = false
13         if(input_utilisateur.length < 20) {
14             Length_ok = true;
15         }
16     }
17     public boolean checkAuth(String loginSaisi, String passwordSaisi) {
18         //... Méthode existante avant l'intervention de SIO-INFO permettant de
19         // vérifier l'authentification des agriculteurs sur l'application GEOMAP.
20         }
21     }
22 }
```

Document 4

Proposition de modification du code source de la page d'authentification de GéoMap par SIO-INFO

```

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  if(SaisieSecurise){
8      //Vérification de l'identité via une requête SQL.
9      if (oneAuth .checkAuth(loginSaisi,passwordSaisi) {
10          //Succès d'authentification, accès au compte privé de l'utilisateur...
11      }
12      else {
13          errMsg.append("Accès refusé, mauvais login et/ou mot de passe.\n");
14      }
15      else {
16          errMsg.append("Saisie non sécurisée.\n");
17      }
18  }
```

Document 5

Politique d'enregistrement des traces recommandée par SIO-INFO

Recommandation : Dans le cadre de la collecte des preuves numériques, tracer les tentatives d'authentification à l'aide du module Logcat (intégré à AndroidStudio) selon la politique suivante :

	Sévérité	Message enregistré dans les logs
Échec d'authentification	Warning	Échec d'authentification utilisateur <login-utilisateur> de <ip-connexion> à <date-heure>.
Succès d'authentification	Info	Saisie utilisateur <login-utilisateur> de <ip-connexion> à <date-heure> non conforme à la politique de sécurité
Saisie non sécurisée	Error	...

Remarque : les informations entre chevrons <> sont à remplacer par des variables.

Document 6

Manuel d'utilisation du module Logcat pour AndroidStudio

La classe **Log** permet de créer des messages de journal qui apparaissent dans Logcat. La méthode à appeler correspond à la première lettre du niveau de严重性 souhaité. Le niveau de严重性 correspond au type d'alerte levé (warning, error, info).

Log.w(String, String) pour enregistrer un message avec la严重性 warning.

```
private static final String TAG = "GEOMAP";
String testVar = "John Doe" ;
Log.w(TAG, «Message de»+testVar);
```

Enregistre le message suivant :
warning : GEOMAP : Message de John Doe.
Le caractère + permet de concaténer des chaînes de caractères.

Document 7

Autres méthodes disponibles dans AndroidStudio

Récupération de la date	Récupération de l'adresse IP
Date date = Calendar.getInstance().getTime(); DateFormat dateFormat = new SimpleDateFormat("dd-mm-yyyy hh:mm:ss"); String recupDate = dateFormat.format(date);	String recupIP = request.getHeader("X- FORWARDED-FOR"); if (recupIP == null) { recupIP = request.getRemoteAddr();}

L'organisation d'une veille technologique

I

Définition

Une **veille technologique** consiste à mener une surveillance sur les développements techniques ou scientifiques, les performances de produits, les résultats de recherche, les applications innovantes (www.enssib.fr).

Elle repose sur un processus regroupant des activités de collecte, de traitement et de partage de l'information.

Les résultats d'une veille technologique doivent permettre de prendre des décisions ou d'orienter des choix technologiques pour bénéficier d'un avantage concurrentiel.

II

Les étapes d'une veille technologique



1. Déterminer les objectifs

La veille technologique est un processus qui mobilise du temps et de l'énergie. Elle doit répondre à un besoin clairement identifié.

Exemple : Une société est régulièrement l'objet d'attaques de type *ransomware* depuis Internet. Elle désire trouver une solution pour repérer et bloquer ce type d'attaques.

Besoin identifié : La société doit améliorer la sécurité de son SI pour éviter des attaques de type *ransomware*.

Objectif de la veille technologique : Suivre l'organisation de ce type d'attaque et les évolutions technologiques dans le domaine des pare-feux afin de trouver une solution adaptée au besoin.

2. Collecter les informations

Les sources d'informations sont très diverses (revues, ouvrages, vidéos, bases de données...). Il convient de commencer sa veille par des sources d'informations générales sur le sujet pour mieux cerner les contours de la problématique. Ensuite, des sources plus précises aident à affiner le travail de recherche. La qualité des résultats d'une veille technologique repose essentiellement sur la qualité et la pertinence des informations collectées.

- La qualité de l'information peut être évaluée par plusieurs critères :

La crédibilité de l'auteur

Elle est mesurable par la vérification de l'expertise de l'auteur et du sérieux de l'organisme à l'origine de la diffusion de l'information.

La fiabilité de la source

Il s'agit de vérifier la qualité de l'organisme à l'origine de la demande d'information.

L'objectivité de l'information

Ce critère permet d'identifier l'orientation choisie par l'auteur dans son développement. Quel est l'objectif visé par l'auteur qui structure son argumentation ?

L'exactitude de l'information

Il faut croiser plusieurs sources d'informations et vérifier si les résultats convergent.

L'actualité de l'information

L'importance de l'actualité de l'information dépend du sujet de veille. Certaines technologies vieillissent plus rapidement que d'autres.

- Mesurer la pertinence de l'information**

Cela revient à se demander si l'information répond à l'objectif de la veille. Certains éléments du document peuvent aider à vérifier sa pertinence : son titre, son introduction, les titres intermédiaires. Le vocabulaire utilisé doit être adapté au lecteur pour faciliter la compréhension.

3. Traiter les informations

Un travail de curation doit être réalisé sur les informations collectées lors de la phase précédente. Celui-ci doit apporter une valeur ajoutée à l'information brute, par exemple avec l'ajout d'un titre, d'un commentaire ou encore d'un point de vue. C'est une tâche qui ne peut pas être réalisée automatiquement, elle nécessite une intervention humaine.

4. Partager les résultats de la veille

Le partage d'informations est l'objectif final du travail de veille. Le travail du veilleur peut être valorisé à travers différentes plateformes et outils permettant de partager son travail.

Les outils d'une veille technologique

I

Les outils de collecte de l'information

Deux méthodes sont mobilisées pour collecter l'information : la méthode « *pull* » et la méthode « *push* ».

La méthode « *pull* » consiste à « tirer » l'information. L'avantage est de mesurer rapidement la pertinence de l'information puisque le veilleur est actif dans l'acte de recherche. L'inconvénient majeur est qu'elle nécessite de rechercher régulièrement de nouvelles informations, sans automatisation et donc, potentiellement, d'omettre des nouveautés importantes.

La méthode « *push* » consiste à « pousser » l'information. Elle permet d'automatiser la remontée de l'information (avec les flux RSS par exemple). L'avantage est d'être informé régulièrement des nouveautés sur le sujet de la veille. L'inconvénient majeur est de se retrouver face à une masse d'informations difficile à traiter.

1. Les agrégateurs de flux RSS

De nombreux méta-moteurs (exemple : rechercheisidore.fr) proposent aujourd'hui de mémoriser les recherches. Les résultats d'une requête sont associés à un flux RSS. Il suffit d'intégrer ce flux dans un lecteur de flux RSS pour être averti en temps réel d'une nouvelle source disponible.

Exemple : Netvibes (agrégateur personnalisable), Feedly (application sur smartphone).



2. Les alertes par courriel

Un courriel est envoyé lorsque de nouveaux résultats correspondent aux termes de la recherche.

Exemple : Google Alertes est un service qui envoie un courriel ou une alerte lorsqu'une nouvelle page Web correspondant aux mots-clés choisis apparaît dans les résultats de Google.

II Les outils de traitement ou de curation

La curation de contenu est une démarche qui consiste à sélectionner des contenus et à les éditer avant de les partager afin de leur apporter une valeur ajoutée. Les outils permettant de réaliser des cartes mentales ou des schémas heuristiques facilitent l'exploration d'idées et l'organisation des informations.

Exemples d'outils : Scoop-it, PearlTrees ou encore Netvibes.



Les outils de partage et de diffusion des résultats de la veille

La diffusion des résultats de la veille technologique est une stratégie à part entière qui va généralement au-delà de la simple mise à disposition du contenu de la curation.

Les modes de diffusion des résultats de la veille doivent répondre aux habitudes du public visé.

Ainsi le choix de ou des outils à mobiliser est réalisé en fonction de différents critères :

- les caractéristiques des destinataires (individus, groupes, etc.) ;
- les supports que l'on veut mettre en avant (article, vidéo, diaporama, etc.) ;
- les canaux de diffusion (Web, messagerie, site intranet, etc.) ;
- les délais de diffusion déterminés (veille ponctuelle, périodique, etc.).

Exemples :

Outil collaboratif	
Outil de partage de code de développement	
Réseaux sociaux	Facebook, LinkedIn, SlideShare, Twitter, Tweetdeck, les Hashtag  TweetDeck 
Sites Web et wiki	

La virtualisation

I

Le principe de la virtualisation

1. Définition

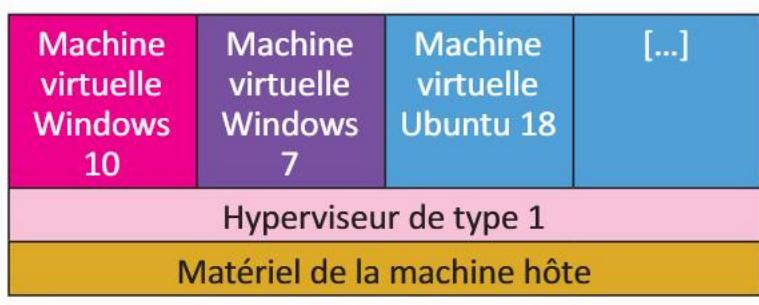
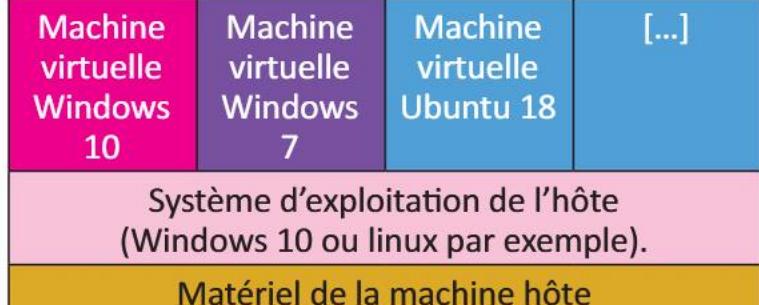
La virtualisation consiste à exécuter sur une machine hôte des systèmes d'exploitation (Windows, Linux...) différents de celui de la machine hôte. La virtualisation repose sur les éléments suivants.

Un système d'exploitation hôte	Il s'agit du système d'exploitation principal qui héberge l'outil de virtualisation et toutes les machines virtuelles. Ce système est hébergé sur une machine physique.	Exemples : Windows, Ubuntu
Un hyperviseur	Il s'agit du logiciel de virtualisation qui permet à plusieurs systèmes d'exploitation différents de travailler sur la même machine physique.	Exemples : VirtualBox, VMWare, KVM
Des machines virtuelles	Ces machines peuvent avoir un système d'exploitation différent et fonctionner en même temps.	Exemples : Windows, Debian

Ainsi, une machine hôte en Windows 10 peut, par exemple, héberger une machine virtuelle sous Linux et inversement.

2. Les deux types d'hyperviseur

Il existe deux types d'hyperviseur :

Hyperviseur de type 1 : natif Un hyperviseur de type 1, ou natif, est un logiciel qui s'exécute directement sur une plateforme matérielle. Exemples : VMWare ESX, Proxmox.	Schéma hyperviseur de type 1 
Hyperviseur de type 2 : hosted Un hyperviseur de type 2 est un logiciel qui s'exécute à l'intérieur d'un autre système d'exploitation. Exemples : VirtualBox, VMWare Workstation.	Schéma hyperviseur de type 2 

L'installation de VirtualBox

VirtualBox est le logiciel de virtualisation utilisé dans certains travaux en laboratoire de cet ouvrage. Pour l'installer, il faut suivre la procédure suivante.

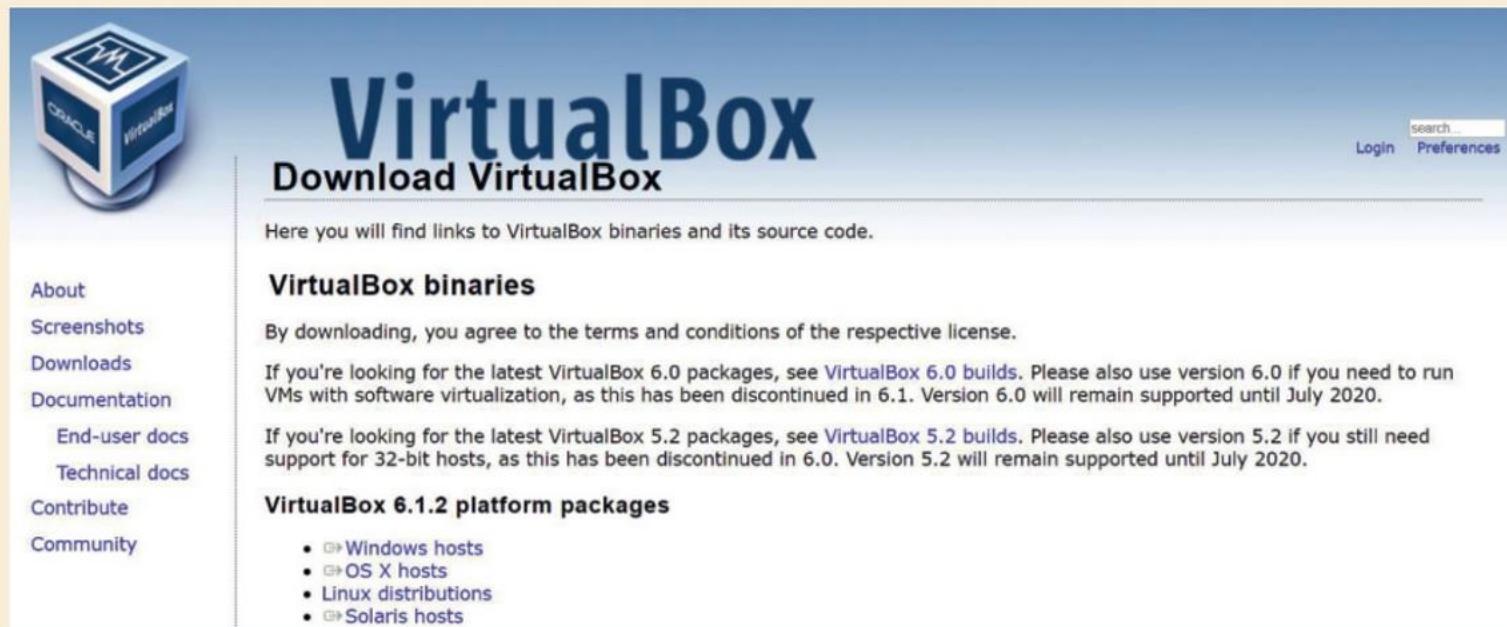
L'utilisation d'un hyperviseur nécessite un ordinateur qui supporte la virtualisation. Il faut aussi vérifier que les fonctions de virtualisation sont activées dans le BIOS. Il convient aussi de disposer de suffisamment de mémoire vive afin que les machines virtuelles et le système hôte puissent fonctionner correctement.

1. Téléchargement

➤  [VirtualBox à télécharger : www.lienmini.fr/6988-001](http://www.lienmini.fr/6988-001)

VirtualBox est un logiciel libre édité par Oracle. Il est téléchargeable gratuitement depuis le site officiel.

Sur Windows, il faut télécharger le fichier d'installation avec l'extension .exe. Pour cela, cliquer sur le lien *Downloads* puis sur *Windows hosts*.



The screenshot shows the official Oracle VirtualBox download page. On the left, there's a sidebar with links: About, Screenshots, Downloads, Documentation, End-user docs, Technical docs, Contribute, and Community. The main content area has a large blue header "VirtualBox Download VirtualBox". Below it, a sub-header says "Here you will find links to VirtualBox binaries and its source code.". There are two main sections: "VirtualBox binaries" and "VirtualBox 6.1.2 platform packages". Under "VirtualBox binaries", it says "By downloading, you agree to the terms and conditions of the respective license." and provides links for "VirtualBox 6.0 builds" and "VirtualBox 5.2 builds". Under "VirtualBox 6.1.2 platform packages", there's a list: "Windows hosts", "OS X hosts", "Linux distributions", and "Solaris hosts". At the top right of the page, there are "Login" and "Preferences" buttons.

Sur Linux, il est possible d'installer directement VirtualBox à partir d'une commande exécutée depuis un terminal (voir ci-dessous).

2. Installation sur une machine hôte

Machine hôte Windows	Double cliquer sur le fichier .exe afin de lancer l'assistant d'installation.
Machine hôte Linux (Debian)	<ol style="list-style-type: none"> Ouvrir un terminal avec la combinaison des touches CTRL+ALT+T Saisir la commande suivante : <code>sudo apt install virtualbox</code> <p>Après validation de cette commande avec la touche ENTRÉE, saisir le mot de passe du compte administrateur afin de lancer l'installation du paquet.</p>

La configuration des machines virtuelles

I

La configuration générale des machines virtuelles

Les options de configurations s'obtiennent en cliquant sur le bouton **Configuration** de chaque machine virtuelle. Les principales options nécessaires pour les travaux en laboratoire sont :

Général	Affiche le nom VirtualBox donné à la machine virtuelle ainsi que le type de système d'exploitation installé.
Système	Configuration de la séquence d'amorçage et choix de la quantité de mémoire vive allouée à la machine. La séquence d'amorçage indique l'ordre dans lequel les périphériques sont testés pour faire démarrer la machine virtuelle (disque dur, lecteur CD, clé USB...).
Stockage	Configuration des unités de stockage (disque dur) avec les contrôleurs IDE et SATA correspondants.

II

La configuration réseau des machines virtuelles

Lors de la création d'une nouvelle machine virtuelle, il y a le choix entre plusieurs types de connectivités réseaux. Les deux principaux types utilisés sont l'accès par pont et le réseau interne.

1. Réseau interne

En réseau interne, la carte réseau virtuelle est associée à un réseau dont il faut choisir le nom. Une liste déroulante permet de sélectionner un nom de réseau déjà existant ou d'en saisir un nouveau.

Avec cette option, les machines virtuelles sont en réseau local, isolées des autres réseaux, à moins de disposer d'un **routeur** qui effectue la liaison entre les différents réseaux internes.

Exemple : Pour un réseau associé à la comptabilité, on peut configurer un nouveau réseau interne nommé *Compta*. Toutes les machines virtuelles associées à ce réseau interne seront liées à un **commutateur** virtuel qui les regroupe dans un même réseau. Il faut cependant veiller à ce que l'adressage IP configuré au sein de la machine virtuelle soit cohérent avec le réseau interne choisi.
Les machines virtuelles sont reliées entre elles mais isolées de l'extérieur.

Réseau interne nommé <i>Compta</i>	
Machine virtuelle 1	Machine virtuelle 2.
Machine physique hôte	

2. Accès par pont

En accès par pont, la carte réseau virtuelle est associée à la carte physique de l'hôte qui héberge VirtualBox. La machine virtuelle accède à la box par la machine hôte qui crée une nouvelle carte réseau (virtuelle) pour celle-ci. Le partage peut s'effectuer *via* la carte filaire ou la carte wifi de la machine hôte.

Exemple : Une machine virtuelle est en accès par pont *via* la carte wifi de la machine physique. La machine virtuelle est vue comme une nouvelle machine appartenant au même réseau que la machine hôte.

Accès par pont <i>via</i> la carte wifi de la machine hôte	
Machine physique hôte	Machine virtuelle

➤ Voir lexique BTS SIO, p. 221



III

Les snapshots

Les *snapshots* (instantanés) permettent d'enregistrer l'état d'une machine à un instant donné, ce qui permet de revenir en arrière en cas d'erreur de configuration ou si la machine virtuelle est endommagée. Il est donc conseillé d'en faire lors des travaux en laboratoire.

Exemple : Lors de la réalisation d'un travail en laboratoire sur une machine virtuelle Windows 10.

Machine virtuelle Windows 10

Snapshot n° 1 : état initial de la machine virtuelle.

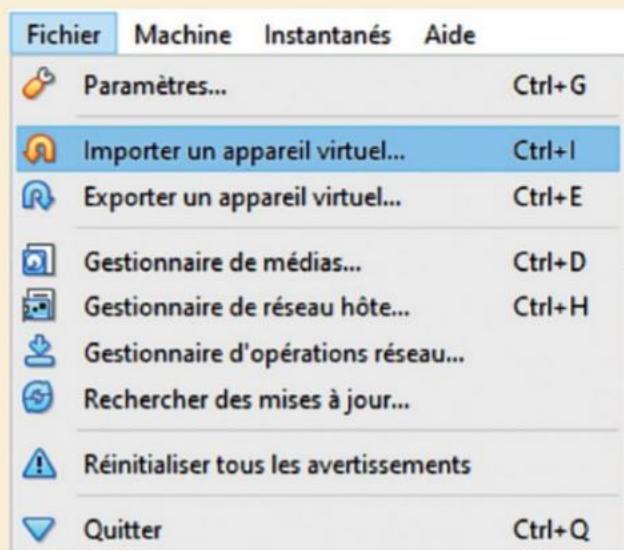
Snapshot n° 2 : état de la machine virtuelle Windows 10 après la fin de la première partie d'un travail en laboratoire.

Lors de la réalisation de la deuxième partie du travail en laboratoire, une erreur de configuration endommage la machine virtuelle Windows 10. Il est alors possible de revenir à l'état correspondant à la fin de la première partie du travail en laboratoire en utilisant le snapshot n° 2 ce qui évite de recommencer l'intégralité du travail.

IV

L'importation de machines virtuelles

La virtualisation permet de réaliser des sauvegardes ou exportations des machines virtuelles pour faciliter le déploiement d'environnements de tests ou la reprise d'activité en cas de cyberattaques.



Il est possible d'importer une machine virtuelle d'un autre environnement de virtualisation dans la mesure où l'on dispose d'une machine virtuelle existante au format *Open Virtualization* (OVF ou OVA).

Pour importer une machine virtuelle, vous devez démarrer VirtualBox et sélectionner successivement les menus « Fichiers » et « Importer un appareil virtuel ».

Les paramètres de la machine virtuelle importée – comme par exemple le lecteur DVD, le contrôleur USB ou encore la carte réseau – peuvent être modifiés à tout moment en cliquant sur le bouton « Machine » puis « Configuration ». Une fois que vous avez vérifié les paramètres, sélectionnez la machine virtuelle importée et dans la barre d'outils, cliquez sur le bouton « Démarrer ».

Paramètres de l'appareil virtuel

Voici les machines virtuelles décrites dans l'appareil virtuel et les paramètres suggérés pour les machines importées. Vous pouvez en changer certains en double-cliquant dessus et désactiver les autres avec les cases à cocher.

<input type="checkbox"/> Processeur	1
<input type="checkbox"/> Mémoire vive	1024 Mio
<input checked="" type="checkbox"/> DVD	
<input checked="" type="checkbox"/> Contrôleur USB	
<input checked="" type="checkbox"/> Carte son	ICH AC97
<input checked="" type="checkbox"/> Carte réseau	Intel PRO/1000 MT Desktop (82540EM)
<input type="checkbox"/> Contrôleur de stockage (IDE)	PIIX4
<input type="checkbox"/> Contrôleur de stockage (IDE)	PIIX4
<input checked="" type="checkbox"/> Contrôleur de stockage (SATA)	AHCI
<input type="checkbox"/> Disque virtuel	Appareil virtuel (appliance)-disk001.vmdk

La méthode EBIOS Risk Manager

I

Présentation de la méthode EBIOS Risk Manager

➤ [Guide de la méthode EBIOS Risk Manager : www.lienmini.fr/6988-002](http://www.lienmini.fr/6988-002)

La méthode EBIOS (expression des besoins et identification des objectifs de sécurité) Risk Manager (RM) est présentée par l'ANSSI comme une « boîte à outils ». Elle donne les lignes directrices pour identifier, analyser et traiter les risques en sécurité de l'information. Il s'agit d'un outil de gestion de risques complet, régulièrement mis à jour et conforme aux référentiels normatifs internationaux.

EBIOS RM repose sur une approche d'appréciation de risques allant du plus global au plus précis. Ainsi, cette approche va du plus simple en termes de scénarios d'attaques, au plus élaboré. Elle vise à obtenir une synthèse entre l'approche par conformité et celle par scénarios.

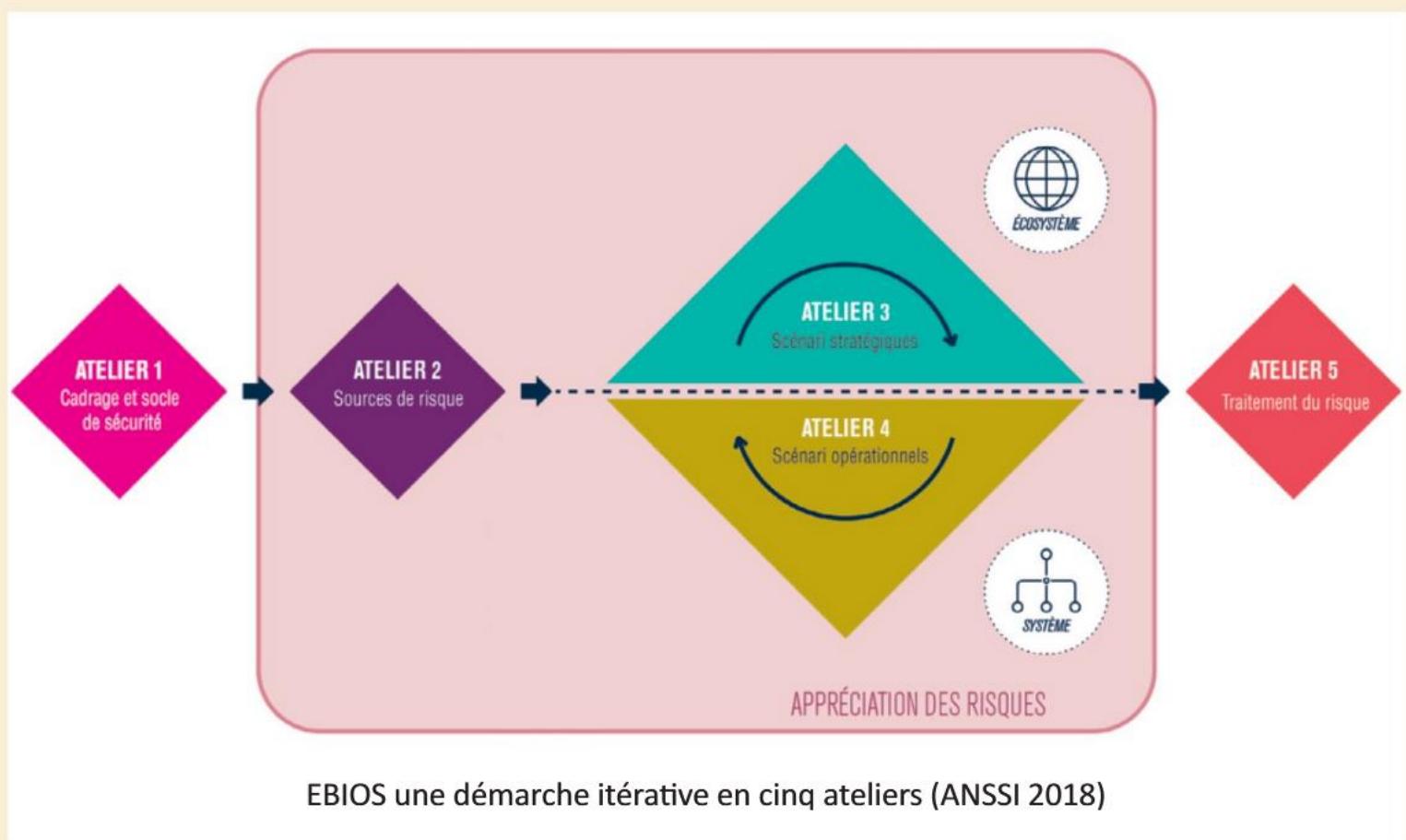
Ainsi, en plus de permettre de conduire une analyse de risque complète et fine sur un processus ou une activité spécifique de l'organisation, elle permet :

- d'identifier le socle de sécurité de l'organisation ;
- d'être en conformité avec les référentiels de sécurité numérique de la CNIL et de l'ANSSI ;
- d'évaluer le niveau de menace de l'écosystème de l'objet de l'analyse ;
- d'identifier les axes prioritaires d'amélioration de la sécurité par la réalisation d'une étude préliminaire du risque.

II

Les étapes de la méthode EBIOS Risk Manager

EBIOS RM consiste en une approche en cinq ateliers. L'approche par conformité est utilisée pour déterminer le socle de sécurité sur lequel s'appuie l'approche par scénarios pour élaborer ceux de risque particulièrement ciblés ou sophistiqués.



1. Atelier 1 : Cadrage et socle de sécurité

ÉCHELLE	CONSÉQUENCES
G4 CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G2 SIGNIFICATIVE	Dégénération des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

EBIOS, niveaux de gravité (ANSSI 2018)

2. Atelier 2 : Sources de risque

SOURCES DE RISQUE	OBJECTIFS VISÉS	MOTIVATION	RESSOURCES	ACTIVITÉ	PERTINENCE
Hacktiviste	Saboter la campagne nationale de vaccination	++	+	++	Moyenne
Concurrent	Voler des informations	+++	+++	+++	Élevée
Hacktiviste	Divulguer des informations sur les tests animaliers	++	+	+	Faible
Cyber-terroriste	Altérer la composition de vaccins à des fins bioterroristes	+	++	+	Faible

L'atelier 1 suit une approche par conformité, ce qui permet d'aborder l'étude du point de vue de la défense. L'objectif de cet atelier, est de recenser les missions, valeurs métier (ou biens essentiels comme un identifiant, un mot de passe, voire les données des utilisateurs) et biens supports relatifs à l'objet étudié (comme un serveur, un poste, un logiciel ou un commutateur). L'atelier vise donc à identifier l'objet de l'étude. Ensuite, il faut identifier les événements redoutés associés aux valeurs métier et évaluer la **gravité** de leur impact.

3. Atelier 3 : Scénarios stratégiques

• Compréhension de l'écosystème

L'atelier 3 permet d'avoir une vision claire de l'écosystème et des menaces. L'écosystème comprend l'ensemble des parties qui gravitent autour de l'objet de l'étude et concourent à la réalisation de ses missions comme des partenaires, des sous-traitants. De plus en plus de modes opératoires d'attaque exploitent les maillons les plus vulnérables de cet écosystème pour atteindre leur objectif, comme par exemple le fait de viser la **disponibilité** d'un service en attaquant le fournisseur de cloud.

➤ Voir lexique BTS SIO, p. 221

- Élaboration de scénarios stratégiques

L'objectif de l'atelier 3 est d'avoir une vision claire de l'écosystème, afin d'identifier les parties les plus vulnérables. Il s'agit ensuite de bâtir des scénarios de haut niveau, appelés scénarios stratégiques. Ces derniers sont autant de chemins d'attaque que pourrait emprunter une source de risque pour atteindre son objectif. Ils sont évalués en termes de gravité. À l'issue de cet atelier, il est déjà possible de définir des mesures de sécurité sur l'écosystème. Les scénarios stratégiques retenus dans l'atelier 3 constituent la base des scénarios opérationnels de l'atelier 4.

SOURCES DE RISQUE	OBJECTIFS VISÉS	CHEMINS D'ATTAQUE STRATÉGIQUES	GRAVITÉ
Concurrent	Voler des informations en espionnant les travaux de R&D en vue d'obtenir un avantage concurrentiel	Trois chemins d'attaque à investiguer. Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données : <ol style="list-style-type: none"> portant directement sur le système d'information de la R&D; sur le système d'information du laboratoire (P3), qui détient une partie des travaux ; passant par le prestataire informatique F3. 	3 Grave

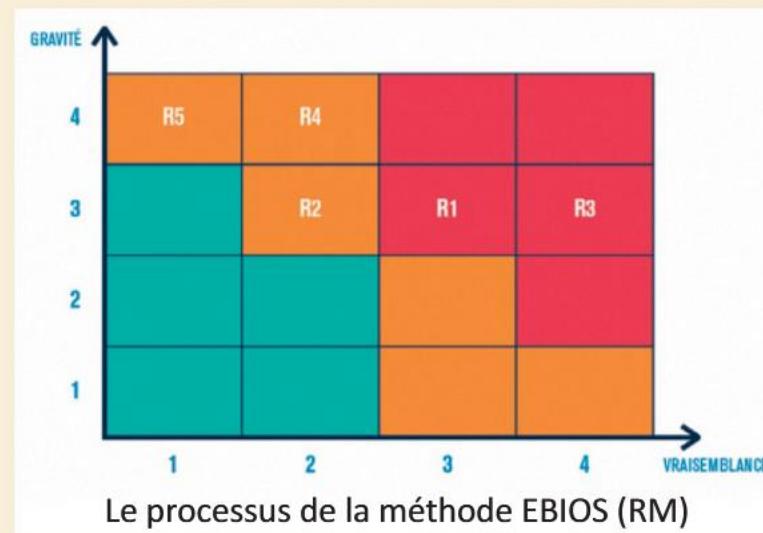
4. Atelier 4 : Scénarios opérationnels

L'objectif de l'atelier 4 est de construire des scénarios opérationnels. Ils schématisent les modes opératoires que pourraient mettre en œuvre les sources de risque pour réaliser les scénarios stratégiques. Cet atelier adopte une démarche similaire à celle de l'atelier précédent mais se concentre sur les biens supports. Les scénarios opérationnels obtenus sont évalués en termes de **vraisemblance**. Cet atelier, permet de réaliser une synthèse de l'ensemble des risques de l'étude.

ÉCHELLE	DESCRIPTION
V4 Quasi certain	La source de risque va certainement atteindre son objectif selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée.
V3 Très vraisemblable	La source de risque va probablement atteindre son objectif selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée.
V2 Vraisemblable	La source de risque est susceptible d'atteindre son objectif selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative.
V1 Peu vraisemblable	La source de risque a peu de chance d'atteindre son objectif selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible.

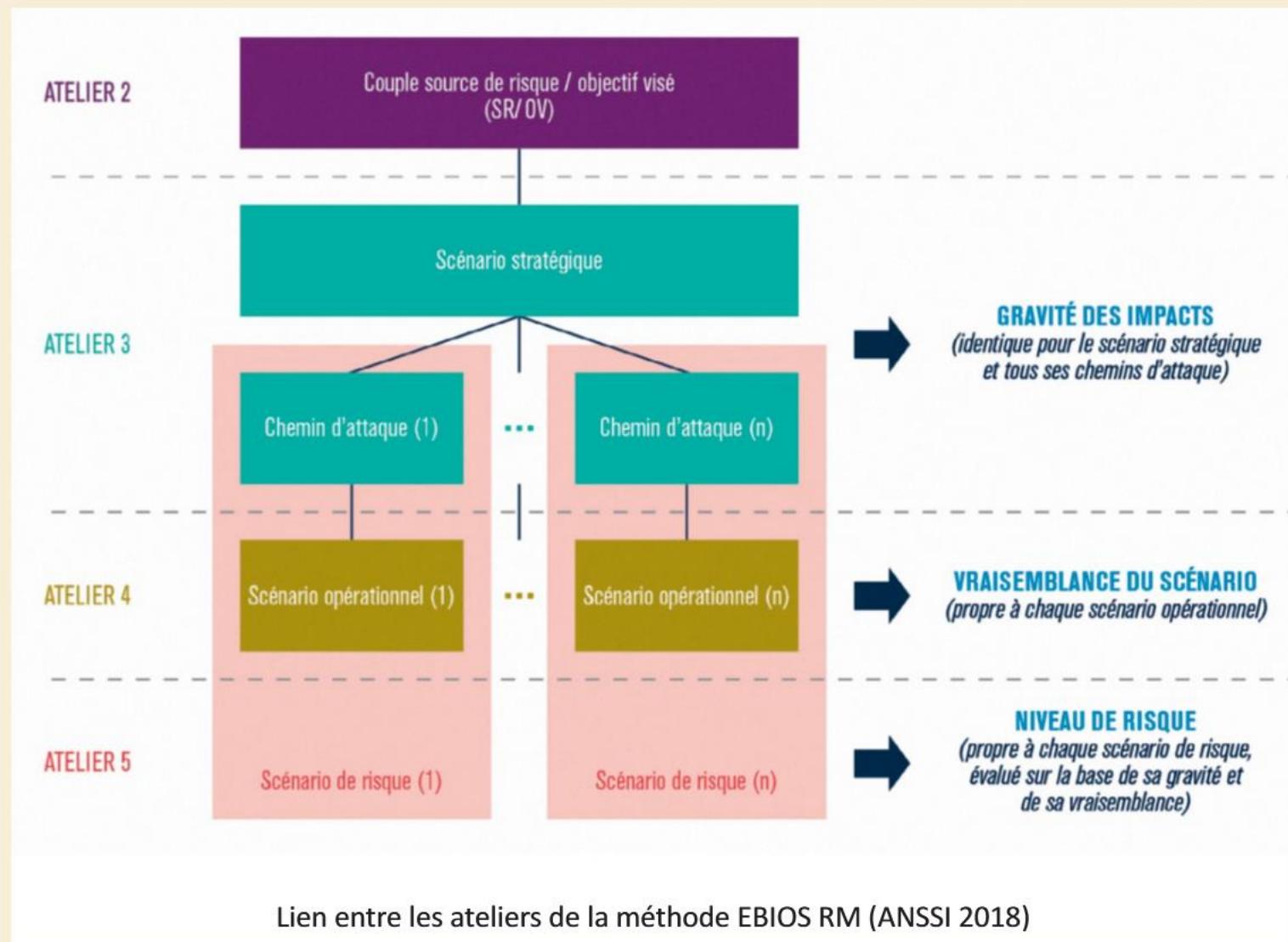
5. Atelier 5 : Traitement du risque

Le dernier atelier consiste à réaliser une synthèse de l'ensemble des risques étudiés pour définir une stratégie de traitement du risque. Lors de cet atelier, on établit la synthèse des risques résiduels et le cadre de suivi des risques est défini.



III

Le processus de la méthode EBIOS Risk Manager



IV

Les différences avec la méthodologie EBIOS 2010

La méthodologie EBIOS Risk Manager apporte quelques variations. Ainsi les modules 4 et 5 de l'étude des risques et des mesures de sécurité de l'EBIOS 2010 se retrouvent dans le cinquième atelier sur le traitement des risques.

Les divergences se retrouvent essentiellement dans les étapes intermédiaires. On ne considère plus les sources de risques intentionnels, les utilisateurs ou les administrateurs sont considérés comme des parties prenantes vulnérables. Par ailleurs, les sources de risques non humaines ne sont plus considérées par la nouvelle méthode.

Le découpage en scénarios stratégiques et opérationnels complexifie la démarche d'analyse mais permet d'offrir une vision globale. Cette approche permet aux dirigeants d'avoir une meilleure compréhension des **vulnérabilités** de leurs organisations et des processus.

Le logiciel Packet Tracer

Le logiciel Packet Tracer est un simulateur de matériel réseau Cisco. Cette application permet de représenter de manière virtuelle le fonctionnement d'un réseau, tout en acquérant des compétences aux technologies spécifiques de Cisco.

I

L'environnement de travail : la barre d'outils

La fenêtre de travail contient deux principales barres d'outils :

- la barre *Objets* pour sélectionner les objets ;



- la barre *Outils généraux* pour apporter des modifications standards sur les objets.



II

Les différents objets

Packet Tracer dispose d'un grand nombre d'objets qui permet de virtualiser la plupart des infrastructures réseaux. Le logiciel permet de «composer» le réseau que l'on veut représenter en choisissant les objets qui le constituent.



III

Les outils généraux

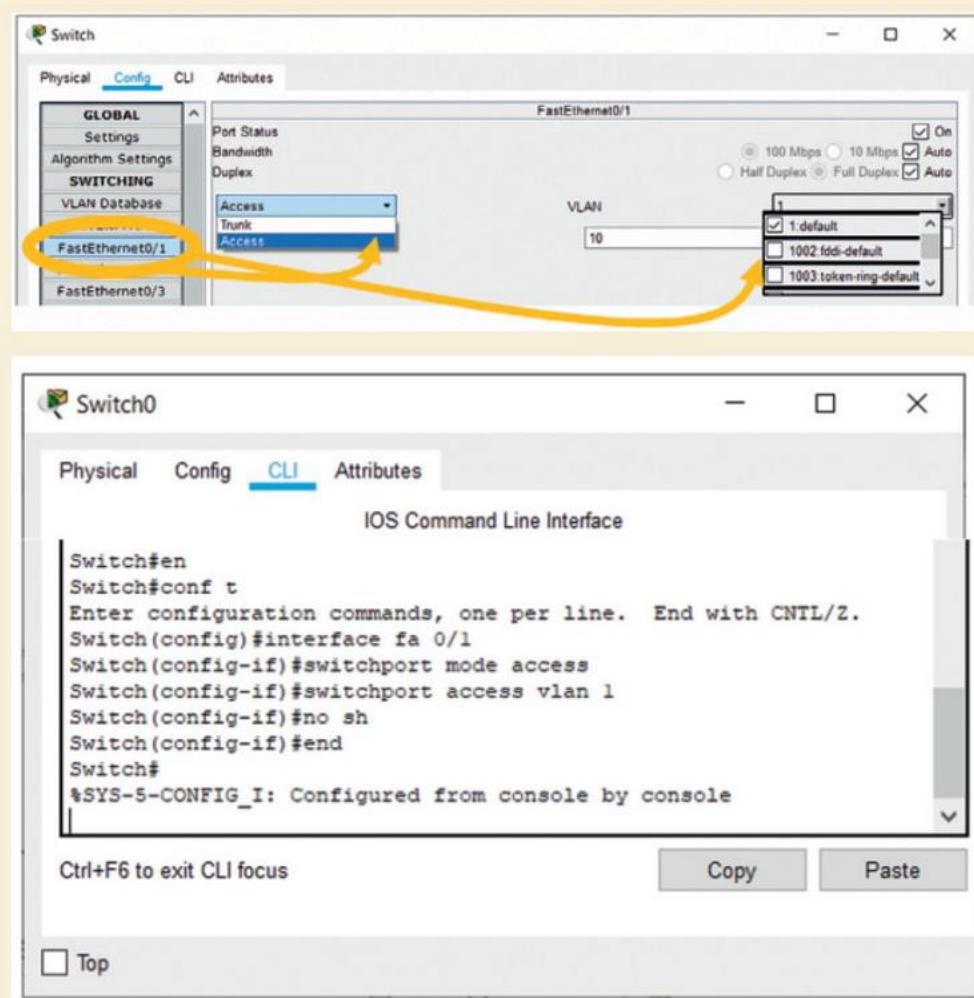
Ces outils permettent d'agir sur les objets réseaux et d'ajouter des commentaires et des formes. Par exemple l'outil *Sélection* active les options de configuration sur un objet, alors que l'outil *Inspection* permet par exemple d'observer la table ARP d'un hôte ou d'un matériel.

Sélection objets	Inspection objets	Suppression objets	Redimensionnement objets	Zone de saisie de texte
Dessiner des formes			Tests des protocoles	

IV

La configuration d'un commutateur

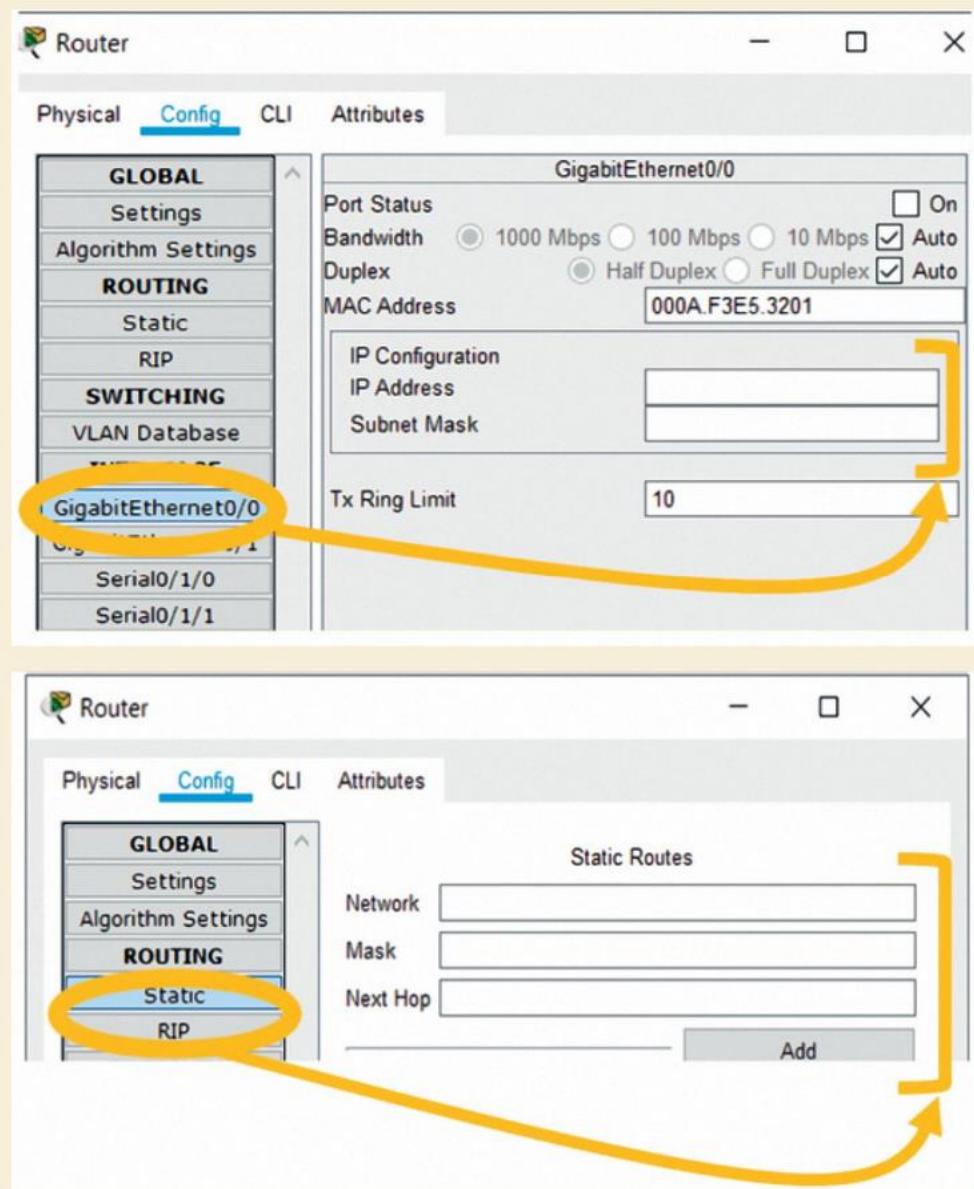
L'onglet **config** permet de configurer le nom d'un **commutateur**, de créer les différents VLANs ou encore affecter ces **VLANs** à des interfaces. L'onglet **CLI** permet également d'apporter des éléments de configuration, mais en ligne de commande. Par exemple l'attribution du mot de passe au mode privilégié (enable) : «enable secret mot_de_passe».



V

La configuration d'un routeur

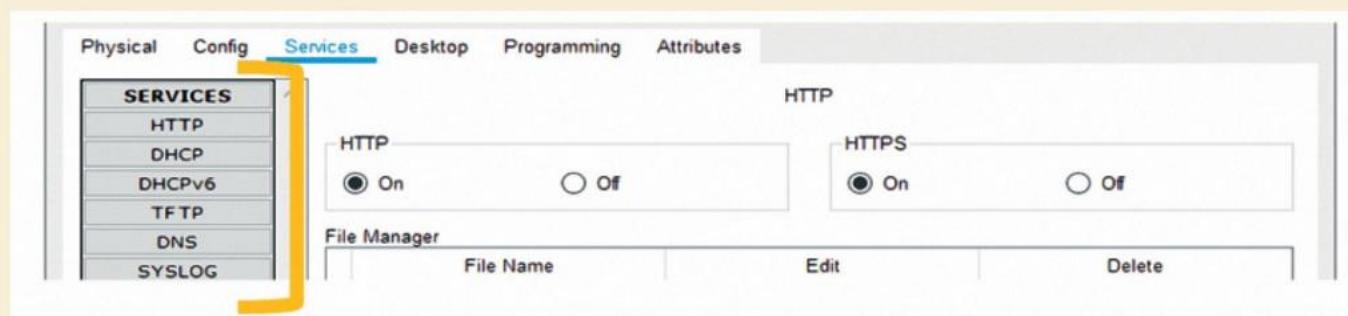
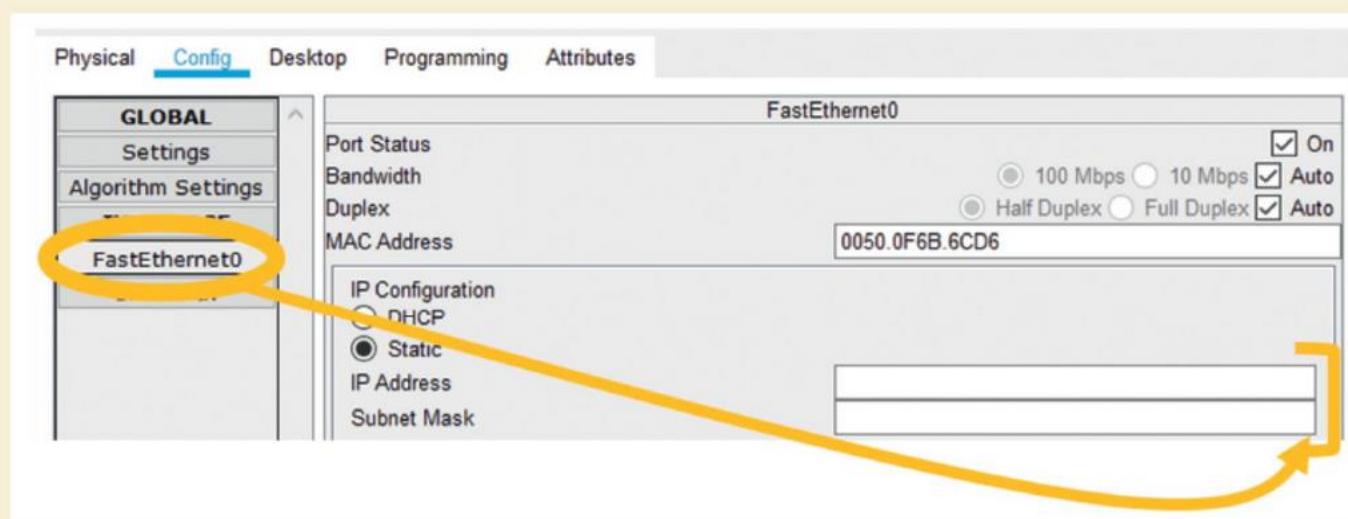
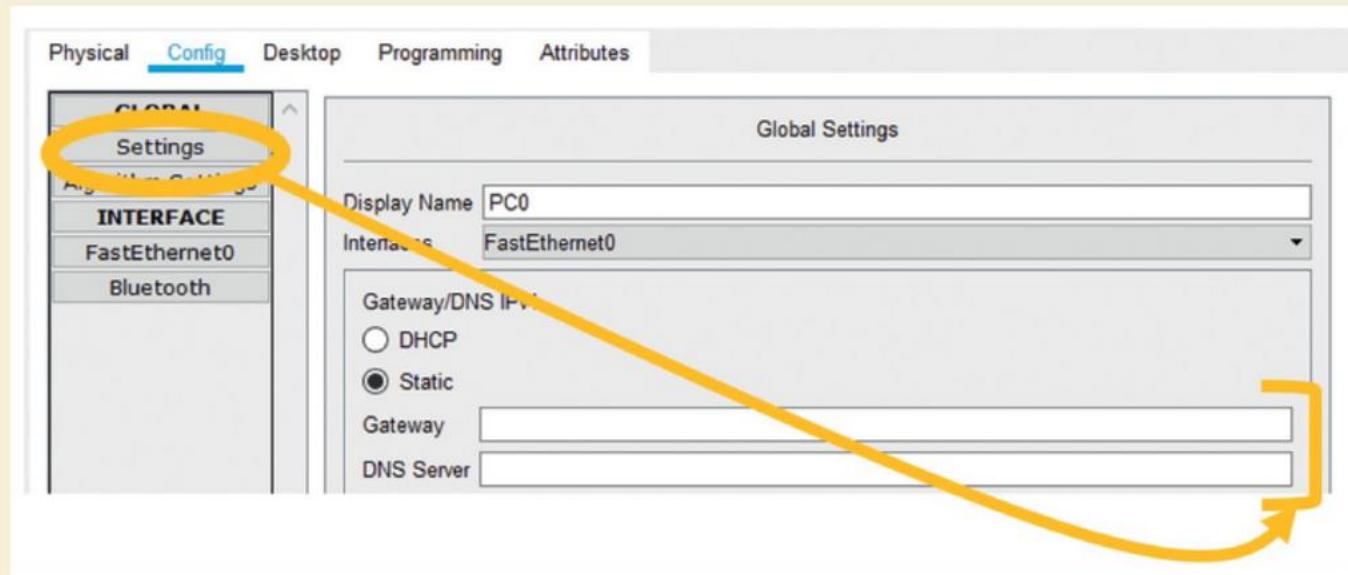
L'onglet **config** permet ici aussi de paramétriser les éléments standards comme le nom ou encore l'adresse **IP** des passerelles. La création des routes est possible avec ce même onglet. L'onglet **CLI** autorise l'ensemble des éléments de configuration en ligne de commande.



➤ Voir lexique BTS SIO, p. 221

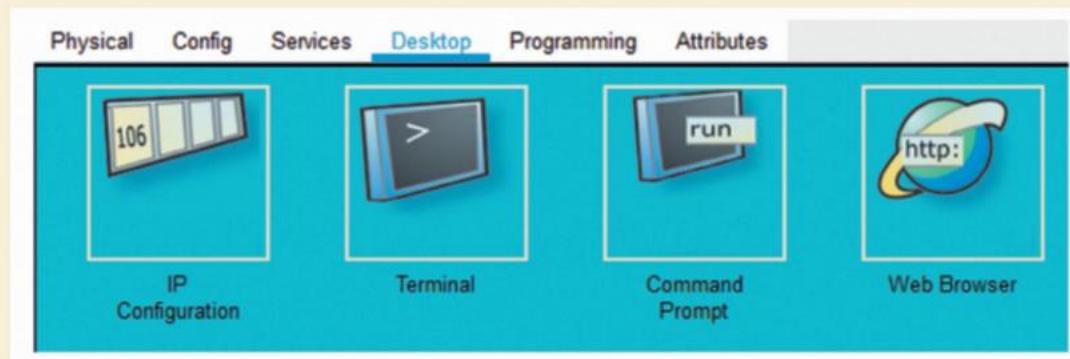
VI La configuration des serveurs et des postes de travail

Packet Tracer permet l'ajout de serveurs et de postes de travail dans l'infrastructure réseau virtuelle. Pour ceux-ci, la configuration du nom et du réseau IP (sous-réseau, passerelle et DNS) est indispensable. Pour les serveurs, l'ajout de services complètera le LAN.



L'onglet **Desktop** permet de vérifier la configuration IP mais également d'utiliser des applicatifs spécifiques comme :

- le **Prompt** pour tester des commandes (exemple : ping) ;
- le **Terminal** pour réaliser une connexion série aux matériels d'interconnexion présents dans le LAN ;
- un navigateur pour exécuter des requêtes http.



➤ Voir lexique BTS SIO, p. 221

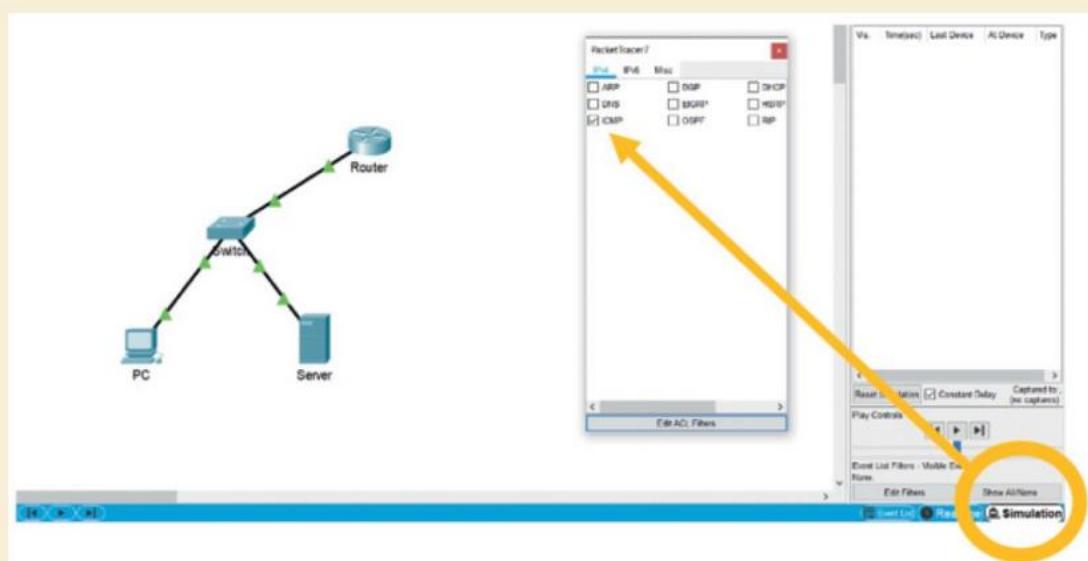
...>

Exemple de test

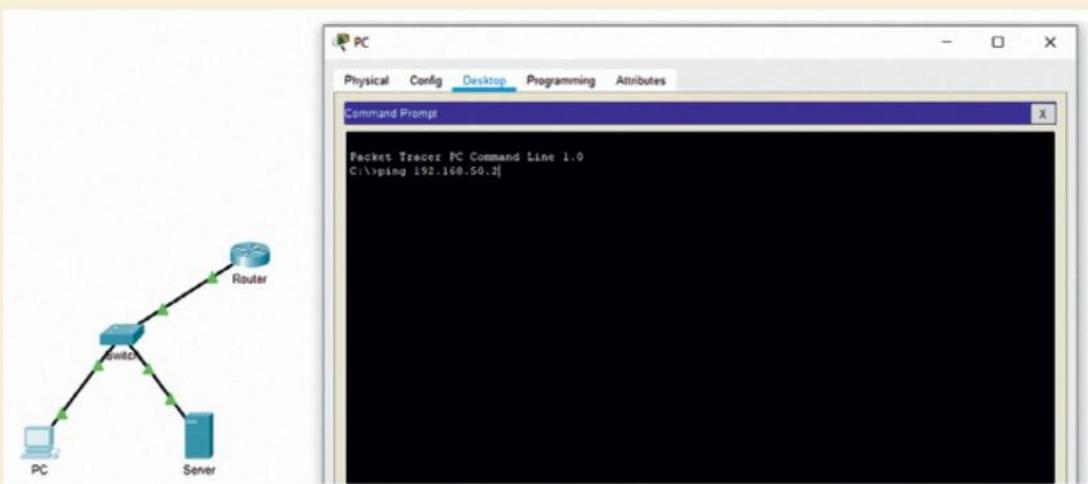
Le mode **simulation** de Packet Tracer permet de tester plusieurs protocoles et ainsi vérifier le bon fonctionnement de l'infrastructure réseau, aussi bien au niveau de la configuration des matériels d'interconnexion que des services proposés.

Exemple : réalisation de la commande PING de PC vers Server :

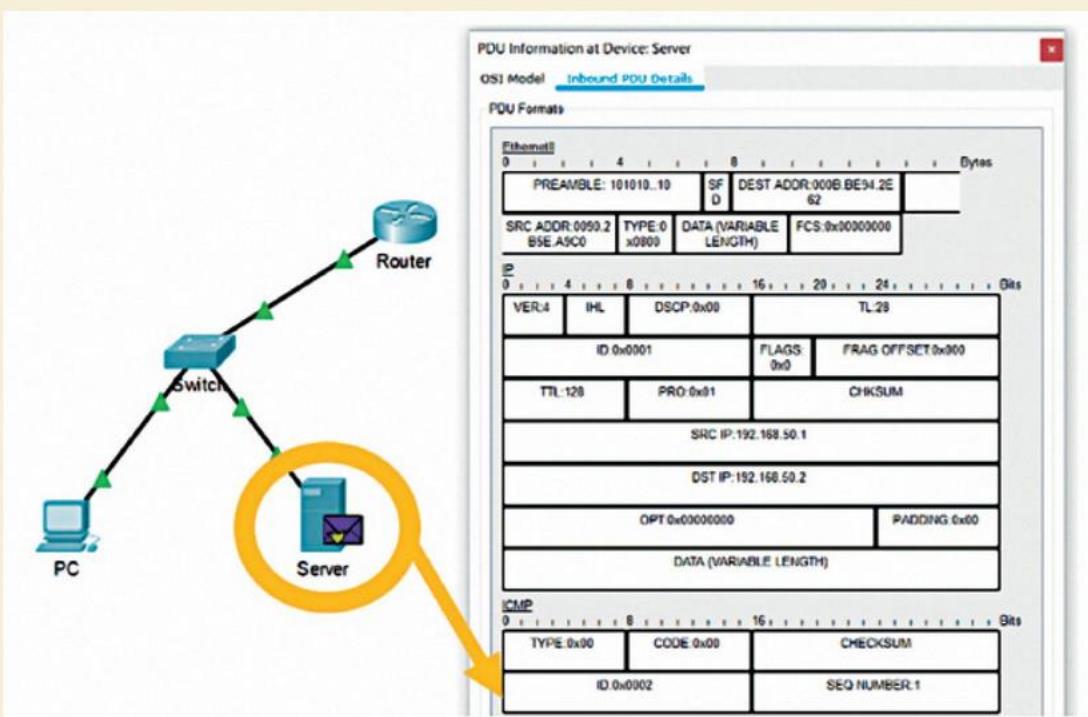
- Choix du protocole ICMP en mode simulation



- Réalisation de la commande ping grâce à l'applicatif **Prompt** sur PC



- Analyse de la trame en cliquant sur l'enveloppe



Le même test peut être réalisé avec l'outil PDU à la place de la commande ping dans le Prompt :



Après avoir sélectionné le protocole ICMP, cliquer sur l'icône PDU puis sur PC et enfin sur Server.

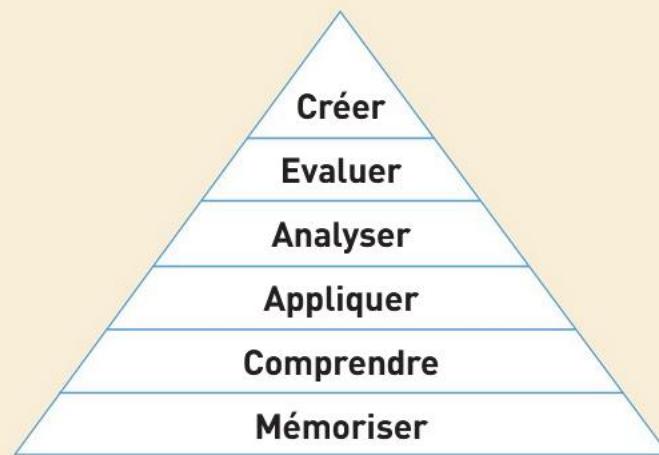
Les consignes de l'épreuve E6

I

La taxonomie de Bloom

La taxonomie de Bloom classe les objectifs d'apprentissage en six niveaux allant du plus simple (le bas de la pyramide), au plus complexe (le haut de la pyramide).

Le questionnement de l'épreuve E6 « Cybersécurité des services informatiques » permet de vérifier le niveau d'acquisition des compétences du bloc 3 associé. Le choix des verbes directeurs permet d'identifier précisément la compétence visée.



II

La compréhension des verbes directeurs

Voici des exemples de verbes directeurs hiérarchisés suivant les niveaux de la taxonomie de Bloom. Cette liste n'est pas exhaustive mais elle permet de cerner la correspondance entre le verbe et les attentes en termes de mobilisation des compétences.

Niveau 1 : Mémoriser

- Un premier niveau de questionnement interroge les compétences liées à la mémorisation des connaissances.
- Verbes directeurs : **définir, décrire, identifier, lister, montrer, collecter, citer**.

Exemple : Identifier une mesure concrète que peut prendre M. Paul au sein du service informatique en faveur de la RSE.

Niveau 2 : Comprendre

- Un deuxième niveau de questionnement interroge les compétences liées à la compréhension des éléments du contexte présenté.
- Verbes directeurs : **interpréter, résumer, distinguer, classer, indiquer, situer, rendre compte, sélectionner**.

Exemple : Classer les menaces de sécurité figurant dans l'extrait du rapport d'audit en fonction des quatre couches du modèle TCP/IP.

Niveau 3 : Appliquer

- Un troisième niveau de questionnement permet d'évaluer si le candidat peut appliquer des méthodes ou principes étudiés en classe.
- Verbes directeurs : **appliquer, changer, démontrer, opérer, montrer, utiliser, résoudre, calculer, compléter, illustrer, examiner, modifier, changer, expérimenter, illustrer, vérifier**.

Exemple : Calculer les coûts annuels de chacune des solutions.

Niveau 4 : Analyser

- Un quatrième niveau de questionnement interroge les compétences d'analyse du candidat.
- Verbes directeurs : **représenter, tracer, relier, associer, analyser, ordonner, expliquer, sélectionner, comparer, différencier, examiner, questionner, tester, étudier, hiérarchiser**.

Exemple : Expliquer en quoi la création d'une vue est une solution pour répondre à ce besoin.

Niveau 5 : Évaluer

- Un cinquième niveau de questionnement mobilise la capacité du candidat à évaluer une situation ou un besoin.
- Verbes directeurs : **critiquer, conclure, synthétiser, déduire, décider, recommander, convaincre, juger, argumenter, défendre, estimer, évaluer, apprécier, considérer, appuyer, justifier.**

Exemple : Justifier le choix de remplacer le serveur physique par une machine virtuelle plutôt que par un nouveau serveur physique.

Niveau 6 : Créer

- Un sixième niveau de questionnement doit vérifier les capacités de création ou de proposition du candidat.
- Verbes directeurs : **créer, inventer, interpréter, concevoir, imaginer, trouver, élaborer, modifier, rédiger, produire.**

Exemple : Rédiger une courte note à destination des membres du groupe de travail proposant des solutions techniques répondant aux questions qu'ils se posent sur l'authentification des usagers.

III

Présentation de l'épreuve

1. Objectif

Cette épreuve vise à évaluer l'acquisition des compétences décrites dans le bloc de compétences « Cybersécurité des services informatiques » :

- protéger les données à caractère personnelles ;
- préserver l'identité numérique de l'organisation ;
- sécuriser les équipements et les usages des utilisateurs ;
- garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques ;
- assurer la cybersécurité d'une solution applicative et de son développement.

2. Critères d'évaluation

Les critères d'évaluation correspondent aux critères de performance exprimés pour chaque compétence du bloc « Cybersécurité des services informatiques » figurant dans le référentiel de certification.

3. Modalités d'évaluation

Cette épreuve ponctuelle écrite dure 4 heures.

Elle revêt la forme d'une étude de cas de production de services informatiques sécurisés, construite à partir d'une situation réelle, mobilisant les ressources décrites pour le bloc « Cybersécurité des services informatiques ». Elle est composée de plusieurs dossiers couvrant différentes missions dans le domaine des solutions logicielles et applications métiers. Elle comporte un dossier documentaire permettant de situer le contexte de l'organisation, les solutions applicatives et d'infrastructure mises en œuvre, les moyens techniques, humains, financiers disponibles, le cadre juridique, l'expression des besoins ayant motivé les services demandés.

La correction est assurée par une personne enseignante en charge d'un bloc professionnel en section de techniciens supérieurs « Services informatiques aux organisations ».

- **ACL (access control list)**

Système permettant de restreindre les accès à un fichier informatique suivant un certain nombre de paramètres.

- **Active directory (AD)**

Mise en œuvre, par Microsoft, des services d'annuaire LDAP pour les systèmes d'exploitation Windows, principalement pour fournir des services centralisés d'identification et d'authentification. Il permet également l'attribution et l'application de stratégies et répertorie les éléments d'un réseau administré tels que les comptes utilisateurs, les serveurs, les postes de travail, les dossiers partagés, etc.

- **ANSSI (agence nationale de la Sécurité des systèmes d'information)**

Autorité nationale en matière de sécurité et de défense des systèmes d'information.

- **Archivage**

Stockage à long terme de documents et de données numériques.

- **Attaques par dictionnaire**

Consiste à trouver un mot de passe en testant une série de propositions prédéfinies dans un fichier, les unes à la suite des autres.

- **Attaques par force brute**

Consiste à tester, une à une, toutes les combinaisons possibles afin de trouver un mot de passe.

- **Attaques par table arc-en-ciel (ou rainbow table)**

Permet de chercher un mot de passe à partir de son empreinte numérique.

- **Authentification**

Mécanisme assurant la vérification de la légitimité d'une demande d'accès.

- **Baie de stockage**

Équipement composé de plusieurs disques regroupés à des fins de stockage.

- **Bandé magnétique**

Support permettant l'enregistrement et la

lecture d'informations analogiques ou numériques.

- **Bandé passante**

Débit binaire maximal d'une voie de transmission.

- **Base de données (ou database)**

Catégorisation des données brutes dans des tableaux. Les données sont classées afin d'être accessibles facilement par l'utilisateur en langage SQL (*structured query language* ou langage structuré de questionnement).

- **Blacklist (ou liste noire)**

Liste d'URLs à bloquer pour permettre un meilleur contrôle de l'utilisation d'Internet. Ces listes sont intégrées dans de nombreux outils de défense comme les pare-feux.

- **Certificat électronique**

Identité numérique d'une organisation vérifiée par une autorité de confiance.

- **CNIL (commission nationale de l'Informatique et des Libertés)**

Commission indépendante chargée de veiller à ce que l'informatique respecte les droits des citoyens.

- **Commutateurs (switch)**

Équipement réseau qui relie plusieurs segments et qui permet de créer des circuits virtuels. Il permet la commutation des trames. Il s'agit d'un boîtier disposant de plusieurs ports RJ45.

- **Confidentialité**

Accessibilité à une donnée après authentification de l'utilisateur.

- **Cookies**

Fichier déposé par le navigateur sur l'ordinateur depuis lequel on navigue sur Internet.

- **Correctifs (ou retouche)**

Section de code ajoutée à une application pour l'améliorer (correction d'un bug, traduction, remédiation à une faille de sécurité, mise à jour, compatibilité, etc.).

- **Défiguration**
Altération de l'apparence d'un site suite à une intrusion illégale sur le serveur web.
- **Délégué à la protection des données (DPO)**
Personne chargée de mettre en œuvre la conformité des traitements avec le RGPD au sein de l'organisme qui l'a désigné.
- **Déni de service**
Rendre un service inaccessible par l'envoi d'une multitude de requêtes vers un serveur pour provoquer sa panne ou sa dégradation.
- **Dénigrement**
Attaque de la réputation d'une personne ou d'une organisation.
- **Diffamation**
Imputation d'un fait non vérifié qui porte atteinte à l'image d'une personne.
- **Disponibilité**
Assurer aux utilisateurs un accès continu à un service ou une architecture réseau.
- **E BIOS (expression des besoins et identification des objectifs de sécurité)**
Méthode d'analyse des risques liés à la sécurité des systèmes d'information.
- **Empreinte numérique**
Procédé technique de calcul permettant de vérifier une source d'information (exemple : MD5).
- **Événement redouté**
Action envisageable sur le système d'information compte tenu des vulnérabilités.
- **Flux RSS (*really simple syndication*)**
Flux d'informations actualisé automatiquement sur le Web après abonnement.
- **Force probante**
Valeur juridique donnée à un mode de preuve.
- **Fraude au président**
Technique frauduleuse qui consiste à se faire passer pour le dirigeant d'une entreprise pour réaliser des actes malveillants.
- **Gravité**
Estimation des conséquences d'un risque informatique.
- **Habilitation**
Capacité légale à exercer certains pouvoirs, à accomplir certains actes.
- **Hameçonnage**
Collecte de données en usurpant l'identité numérique d'une organisation.
- **Identité agissante**
Traces laissées sur Internet par l'organisation lors de ses navigations ou de ses apparitions permettant de l'identifier.
- **Identité déclarative**
Données que l'organisation choisit de partager sur Internet.
- **Identité numérique**
Ensemble des contenus diffusés sur Internet permettant d'identifier une organisation.
- **IDN (*internationalized domain name*)**
Nom de domaine unique d'une organisation sur Internet.
- **Imputabilité**
Possibilité d'attribuer la responsabilité d'un acte à une personne clairement identifiée.
- **Incident**
Tout évènement qui ne fait pas partie du fonctionnement standard d'un service et qui peut causer une interruption ou une diminution de la qualité de ce service.
- **Intégrité**
Assurance qu'il est impossible de modifier des données pendant leur transfert, leur traitement ou leur stockage.
- **IP (*Internet protocol*)**
Numéro permettant d'identifier un hôte (exemples : ordinateur, imprimante, smartphone) sur un réseau informatique.
- **IPS (*intrusion prevention system*)**
Outil qui permet de détecter et de bloquer automatiquement des attaques informatiques.
- **KERBEROS**
Protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le

risque d'interception frauduleuse des mots de passe des utilisateurs.

- **LAN (local area network)**

Réseau informatique local qui permet à des hôtes de communiquer au sein d'une organisation sans utiliser d'accès à Internet.

- **LDAP (light weight directory access protocol)**

Protocole permettant l'interrogation et la modification des services d'annuaire, devenu une norme pour les systèmes d'annuaires. C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs.

- **Menace**

Cause intentionnelle ou non intentionnelle qui peut entraîner des dommages sur le système d'information.

- **NTFS (new technology file system)**

Système de fichiers développé par Microsoft. NTFS est le successeur de FAT et dispose de nombreuses améliorations comme l'utilisation d'extensions supplémentaires, les listes de contrôles d'accès (ou ACL) et la journalisation des fichiers.

- **NTP (Network Time Protocol)**

Protocole qui permet de synchroniser l'horloge des ordinateurs et des serveurs.

- **Passphrase (passe de phrase ou phrase secrète)**

Désigne un mot de passe d'un nombre important de caractères qui contient des suites de mots qui ressemblent à une phrase pour des raisons mnémotechniques.

- **Patch**

Référence corrective.

- **Pentester**

Réalise des tests d'intrusion pour tester la sécurité des systèmes d'information et propose des solutions pour réduire leur degré de vulnérabilité.

- **PHP**

Langage de programmation utilisé pour la production de pages web.

- **Privilège**

Délégation d'autorité sur un système informatique. Il permet à un utilisateur d'effectuer une action : créer un dossier, lire ou supprimer un fichier, etc.

- **Processus métier**

Dans le prolongement de la définition de l'ISO 9000 : 2000, un processus métier est un « ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie » dont l'objectif est de répondre à un besoin client.

- **Proxy**

Machine qui sert d'intermédiaire entre les machines d'un réseau local et d'un réseau distant (WAN ou Internet). Il participe à la sécurité du réseau local en filtrant les contenus Web et les malwares.

- **Registre des activités de traitements**

Registre qui recense les traitements réalisés sur les données à caractère personnel.

- **Responsable du traitement des données**

Personne qui met en œuvre les mesures de sécurité des locaux et des systèmes d'information et qui fixe une durée raisonnable de conservation des informations personnelles.

- **RGPD (règlement général sur la protection des données)**

Texte européen de référence en matière de protection des données à caractère personnel.

- **Risque**

Probabilité de l'exploitation d'une vulnérabilité du SI par une menace.

- **Routeur**

Équipement réseau qui permet le routage des paquets IP. Il permet de faire transiter des paquets d'une interface réseau vers une autre selon un ensemble de règles. On parle aussi de passerelle vers un réseau distant ou réseau différent du sien.

- **SAM (security account manager)**

Base de données des comptes locaux sur le système d'exploitation Windows. Elle contient les identifiants et les mots de passe. Ces données sont « hachées » en MD5.

- **Serveur Web**

Serveur informatique qui héberge des sites Web.

- **Signature**

Portion de code d'un virus informatique. Elle permet à un logiciel antivirus de confirmer la présence d'un virus et de l'identifier. Elles sont présentes dans les bases de signatures des antivirus.

- **Signature électronique**

Signature numérique réalisée à partir de la cryptographie qui permet d'imputer une action à une personne.

- **SSL (*secure sockets layer* ou **couche de sockets sécurisée**)**

Protocole permettant de créer un canal sécurisé pour les échanges sur les réseaux informatiques. Sur les navigateurs, son utilisation est visible par l'apparition d'un cadenas.

- **Système de fichiers**

Désigne soit l'organisation hiérarchique des fichiers au sein d'un système d'exploitation, soit l'organisation des fichiers au sein d'un volume physique ou logique.

- **TLS (*transport layer security*)**

Protocole de sécurisation des échanges sur Internet.

- **Traçabilité**

Dispositif permettant de visualiser un historique des actions.

- **Traitement**

Toute opération ou tout ensemble d'opérations portant sur des données, quel que soit le procédé utilisé.

- **Usurpation d'identité**

Prendre l'identité d'une autre personne pour réaliser des actions frauduleuses.

- **VLAN (*virtual local area network* ou **réseau local virtuel**)**

Réseau informatique logique indépendant.

- **VPN (*virtual private network* ou **réseau privé virtuel**)**

Prolongement du réseau local de l'organisation par une liaison cryptée qui permet d'échanger des données entre deux entités distantes de manière sécurisée via le réseau public Internet.

- **Vraisemblance**

Possibilité qu'une action malveillante ou non aboutisse à l'objectif visé.

- **Vulnérabilité**

Faiblesse de la sécurité du système d'information (SI).

Un livre aux ressources numériques intégrées

OU
Code à flasher

Flashez moi !



OU
Lien URL à saisir



En savoir plus : www.editions-delagrave.fr

Pour compléter votre formation



Cet ouvrage a été imprimé sur du papier provenant de forêts gérées durablement.

DELAGRAVE

www.editions-delagrave.fr



CET OUVRAGE EXISTE AUSSI EN VERSION NUMÉRIQUE

Achat individuel élève disponible sur www.boutique.edulib.fr