CHAPITRE 3

Préserver l'identité numérique de l'organisation

COMPÉTENCES

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

SAVOIRS ASSOCIÉS

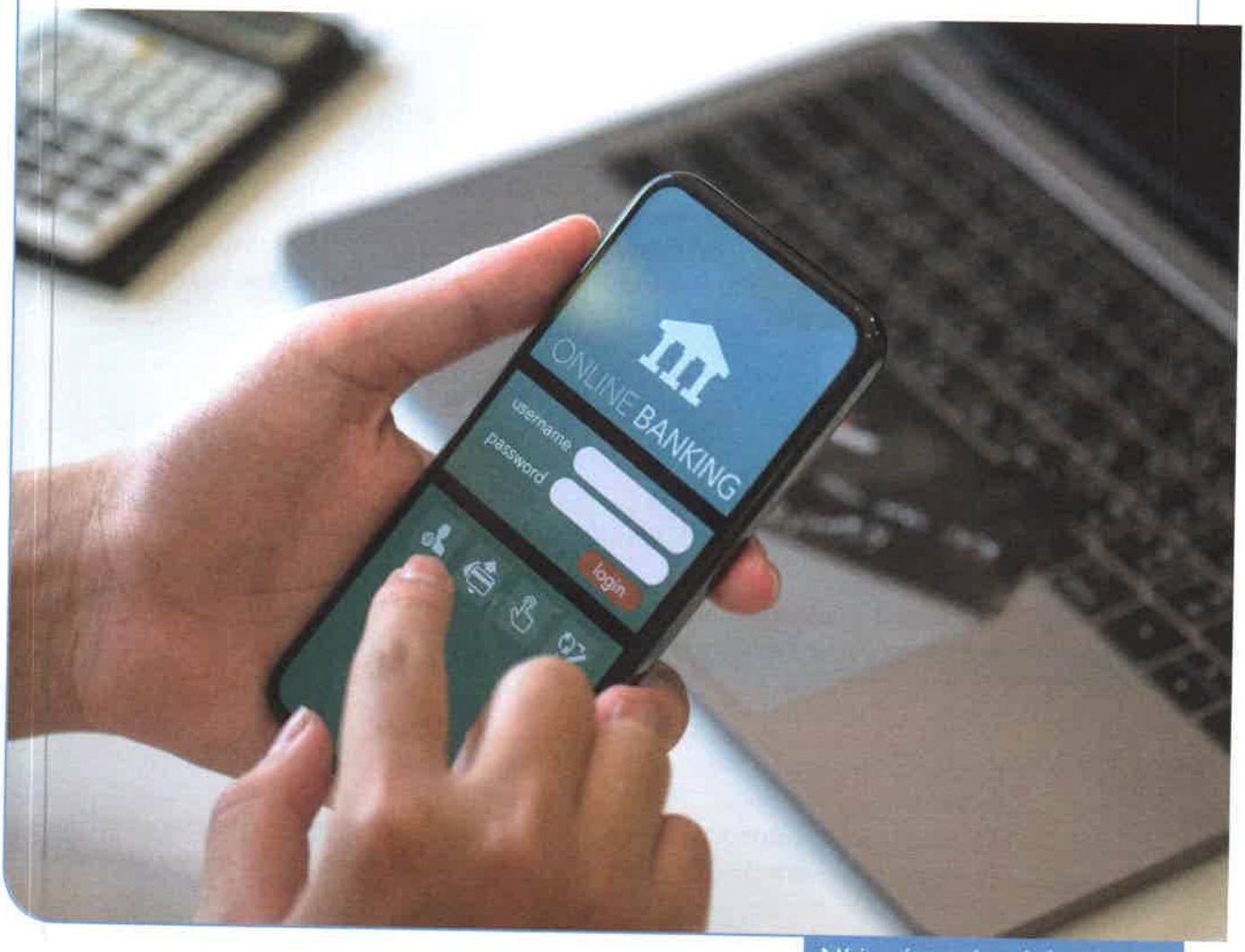
- L'identité numérique de l'organisation : risques et protection juridique
- Droit de la preuve électronique
- Les risques des cyberattaques pour l'organisation : économique, juridique, atteinte à l'identité de l'entreprise

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

CHAPITRE 3

Missions professionnelles

Mission 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 [redacted] 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

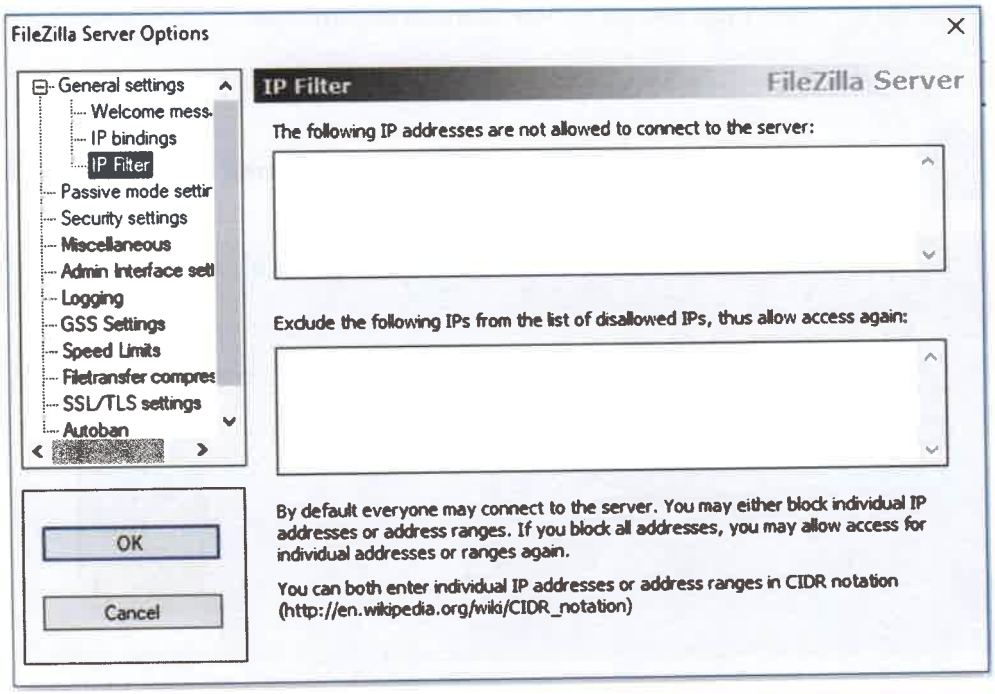
L'apparence du site après sa défiguration

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

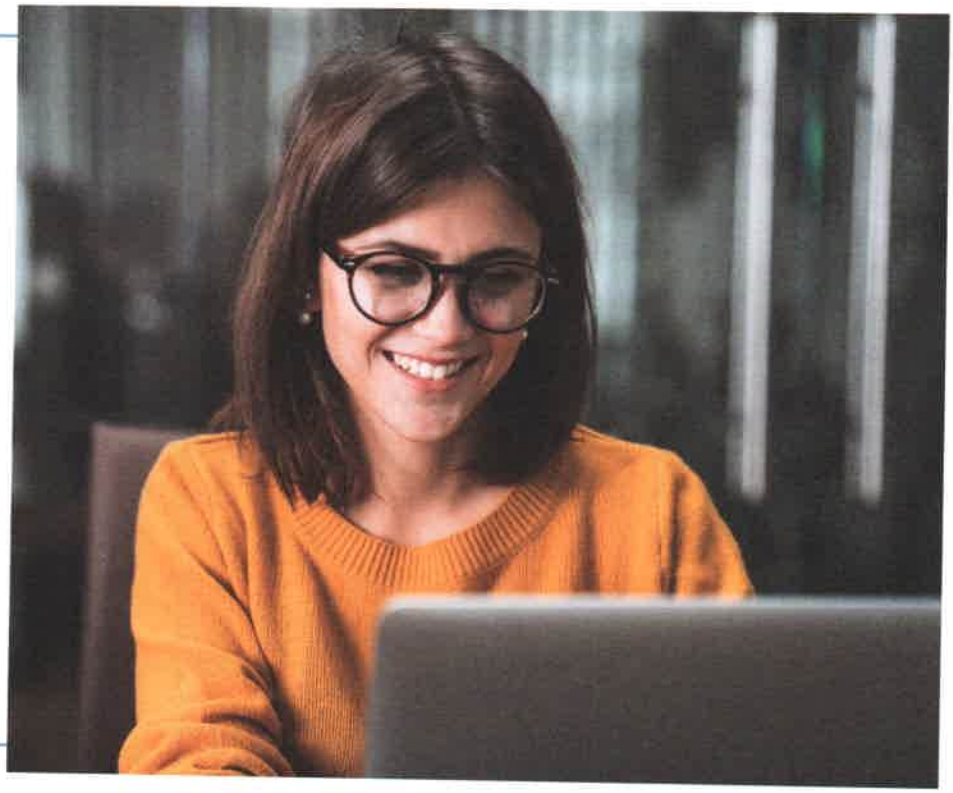
M@Banquea été victime d'une rumeur négative (*bad buzz*) lorsque les clients ont constaté la défiguration de son site commercial.
Les messages postés sur Twitter à propos de M@Banque peuvent être préjudiciables pour l'entreprise.

Missions professionnelles

Mission 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. M^me^ 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

CHAPITRE 3

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.

Courriel envoyé par la personne A vers la personne B

Courriel reçu par la personne B depuis la personne A

D'après « Comment assurer le chiffrement de vos emails avec PGP », www.ionos.fr, 9 octobre 2019.

> Voir lexique BTS SIO, p. 221

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.

CHAPITRE 3

Travaux en laboratoire informatique

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	Crédibilité 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
Malware		
Spam		
...		

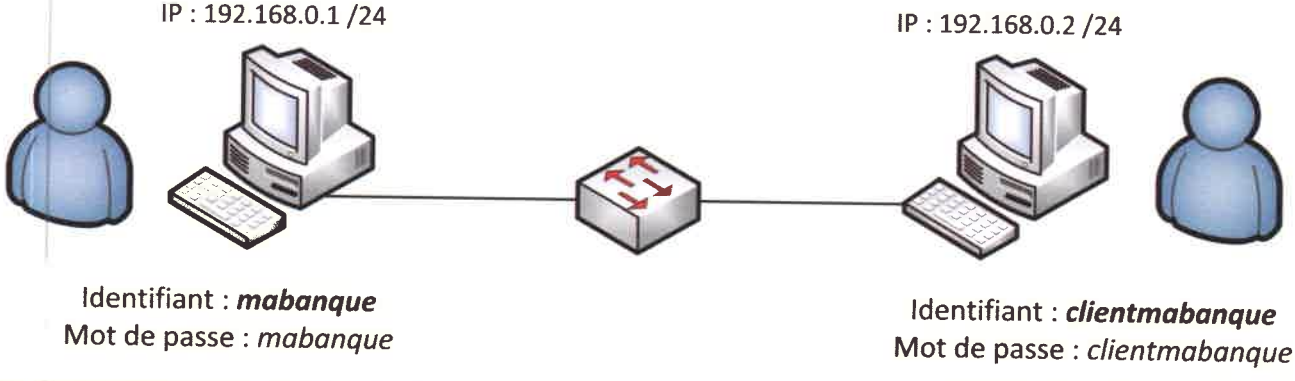
2 Déployer des moyens de preuves sécurisés et conformes à la législation

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.

   > Document 2
3. Testez l'envoi de courriels entre les deux acteurs et vérifiez si le contenu du message est crypté.
   > Document 3
4. Téléversez les clés publiques sur un serveur de clés dédié afin d'assurer le cryptage du contenu des messages.
   > Document 4
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

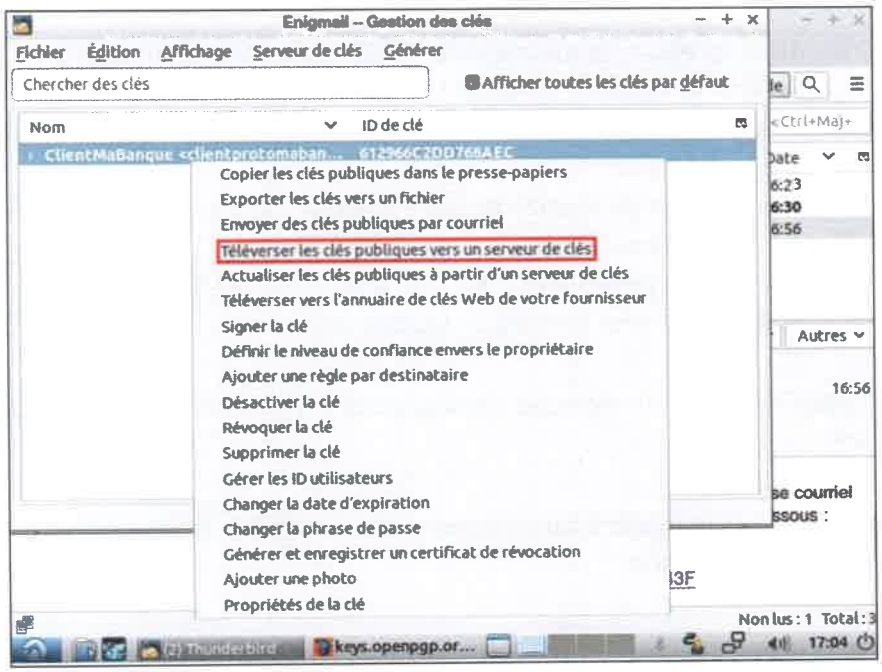


Document 2 Le cahier des charges de l'environnement de tests

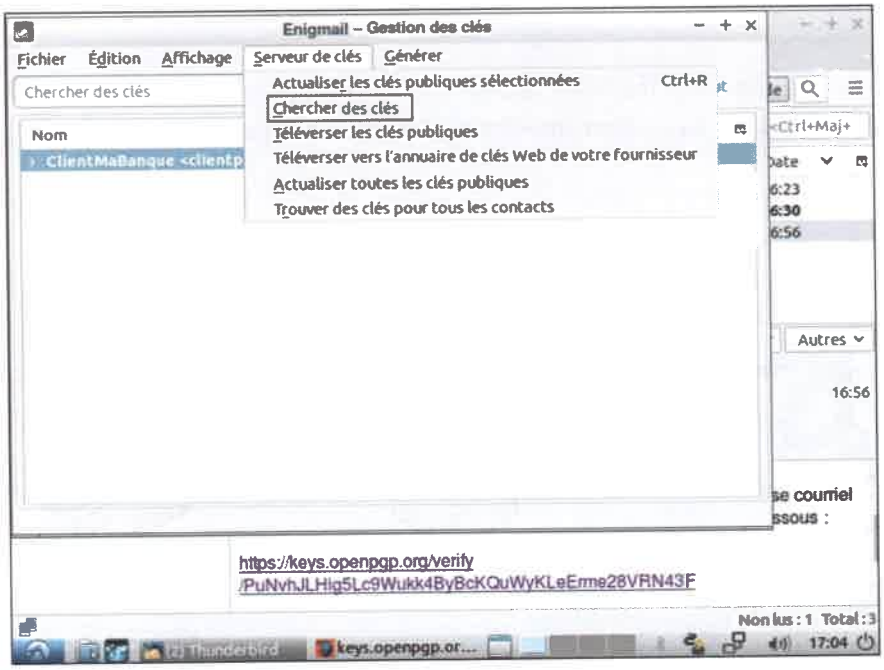
Machine virtuelle « M@Banque »	**Machine virtuelle** « client de M@Banque »
Système d'exploitation : Debian	**Système d'exploitation :** Debian
Client de messagerie : ThunderBird	**Client de messagerie :** ThunderBird
Nom du compte de messagerie : MaBanque	**Nom du compte de messagerie :** ClientMaBanque
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



CHAPITRE 3

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.	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.	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 : un article publié sur le site de l'organisation.	**Exemple :** les consultations de sites Internet pour la recherche d'un nouveau fournisseur par un membre de l'organisation.	**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 (*Internationalized Domain Name*, « 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 [redacted].	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
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. **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. 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.	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. 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.

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

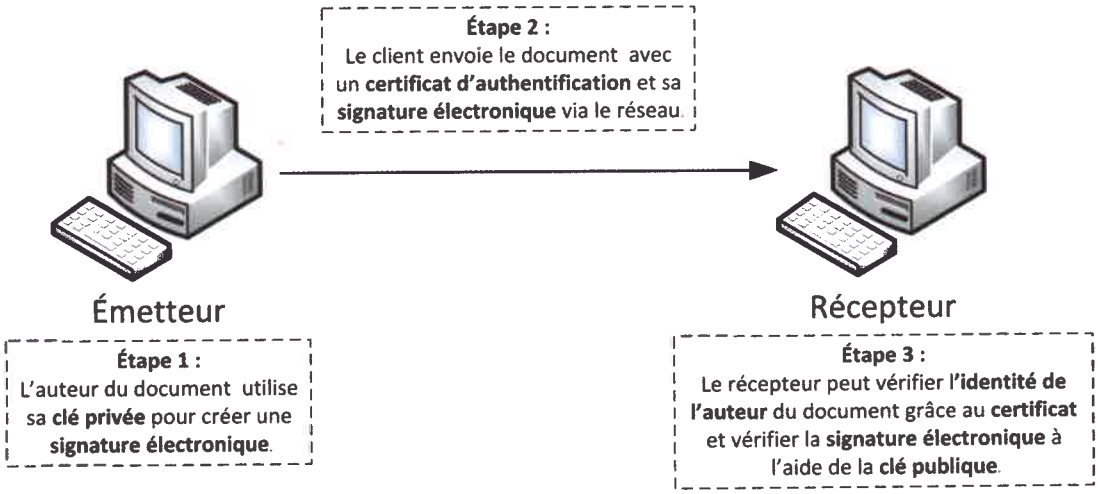
1. Les moyens/supports de l'authentification

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 décrypter.
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. C'est un début de preuve si la loi exige un écrit « parfait ».	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 ».

Fiche savoirs CEJM appliquée 5

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.

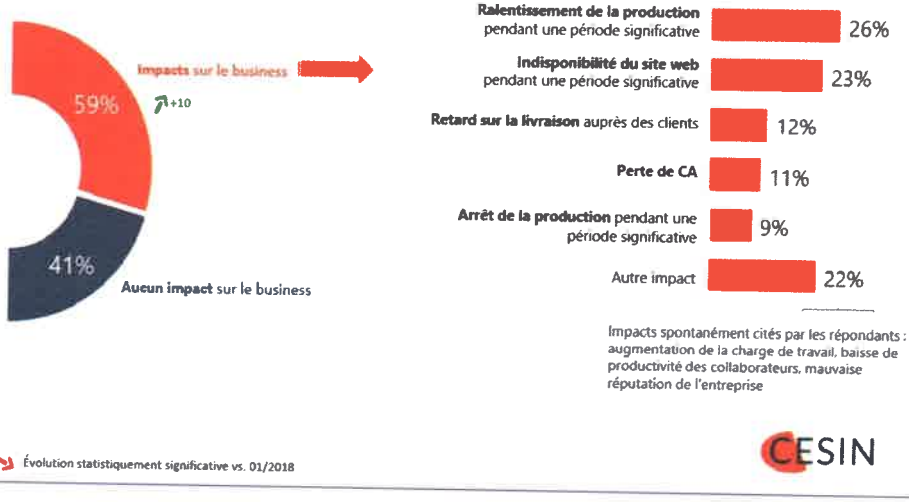
I Les risques économiques des cyberattaques

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.

Extrait de l'enquête du CESIN sur l'impact des cyberattaques pour une organisation

Q30. Quel a été l'impact des cyber-attaques sur votre business ?
Base : ensemble (174 répondants) / Plusieurs réponses possibles



2. Le calcul économique du risque acceptable

La prise en compte des risques découle des résultats d'une analyse méthodologique (par exemple, la méthode EBIOS, 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

Applications

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

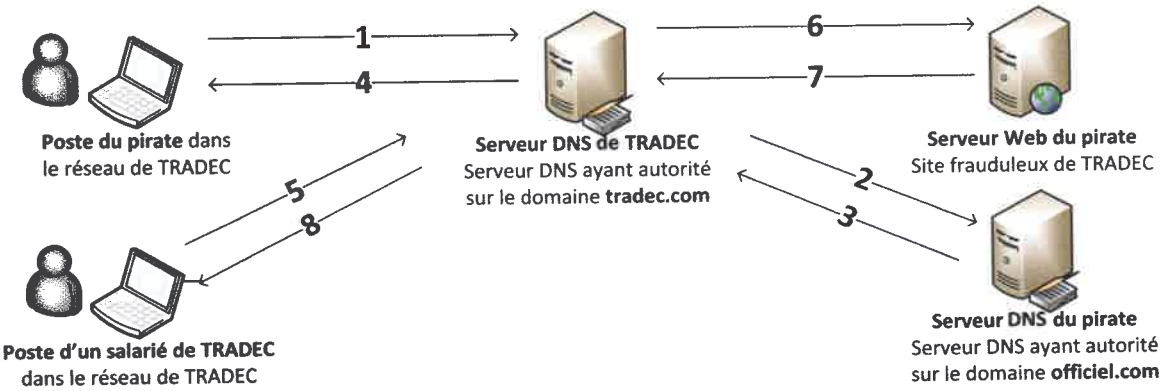
1 Retrouvez la composante de l'identité numérique visée par la cyberattaque de Tradec.

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

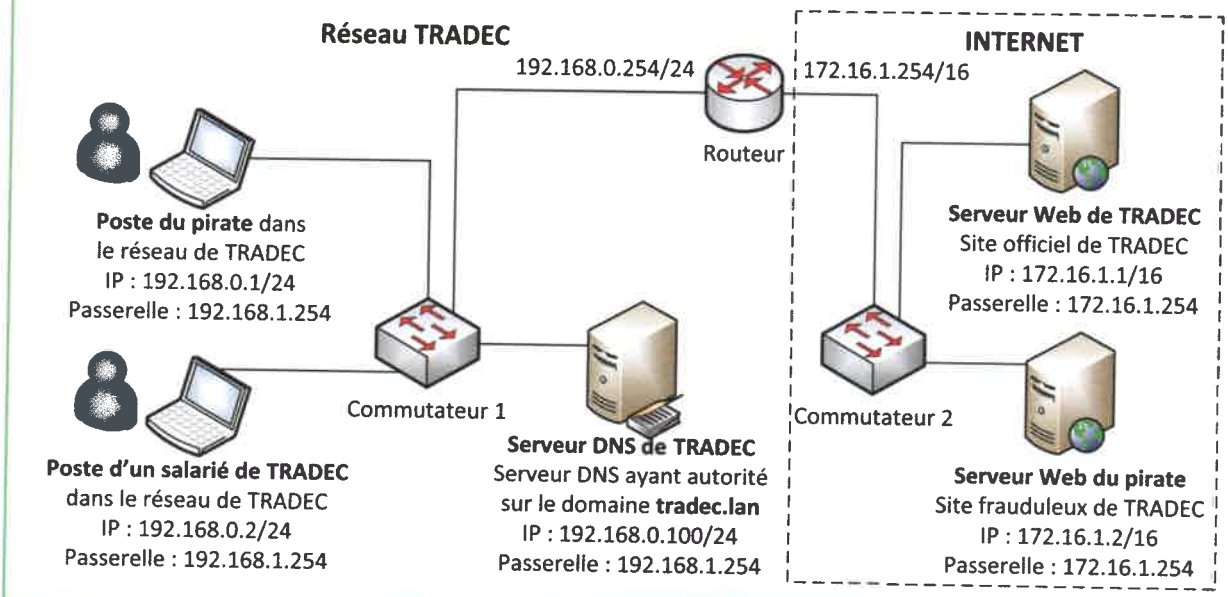
> Fiche CEJMA 3

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 choisirez 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
Comp...Composant 2 Composant 1 TLD

• 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 ;

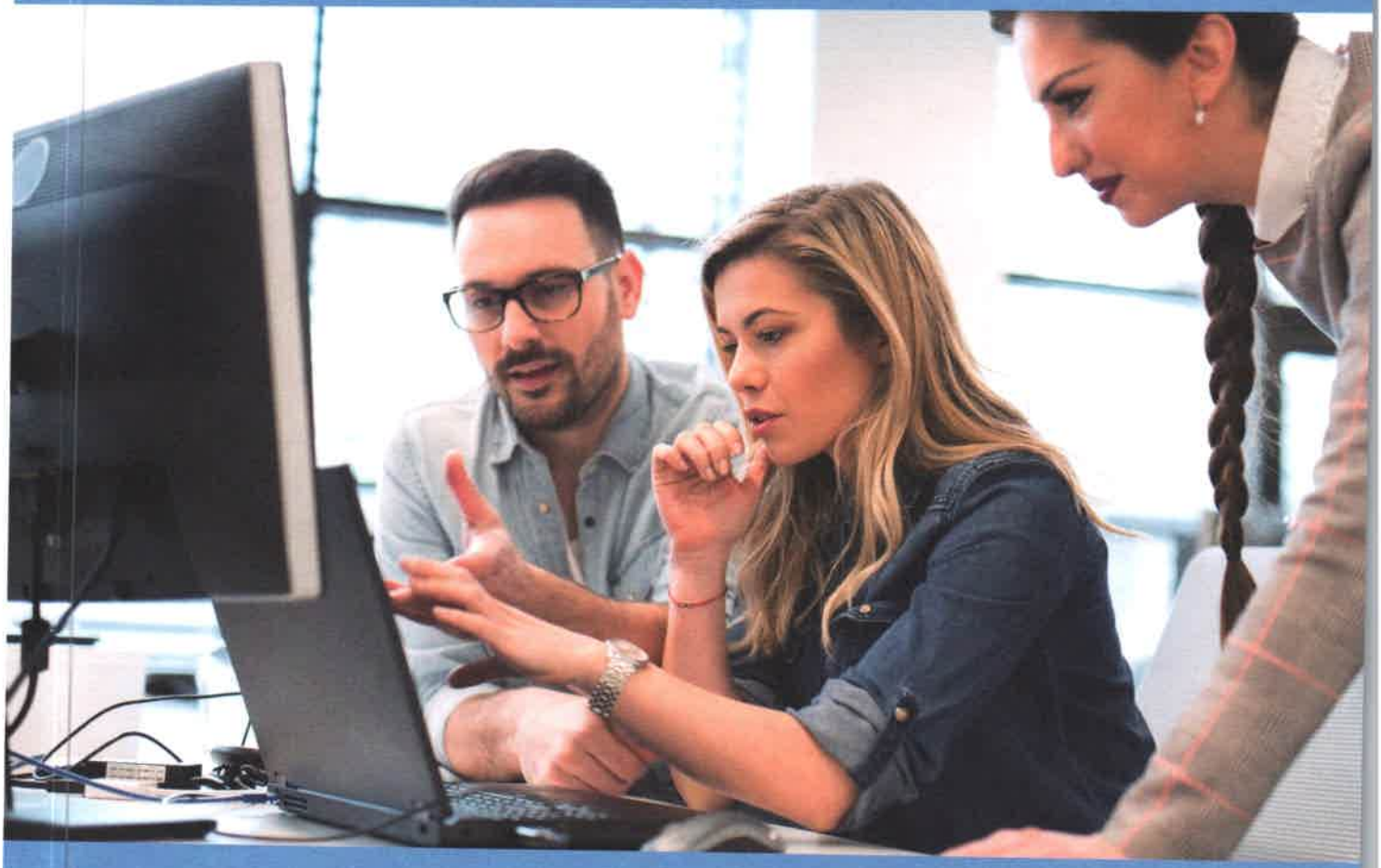
– conservez des captures d'écran du faux profil et de ses publications ;

– 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.

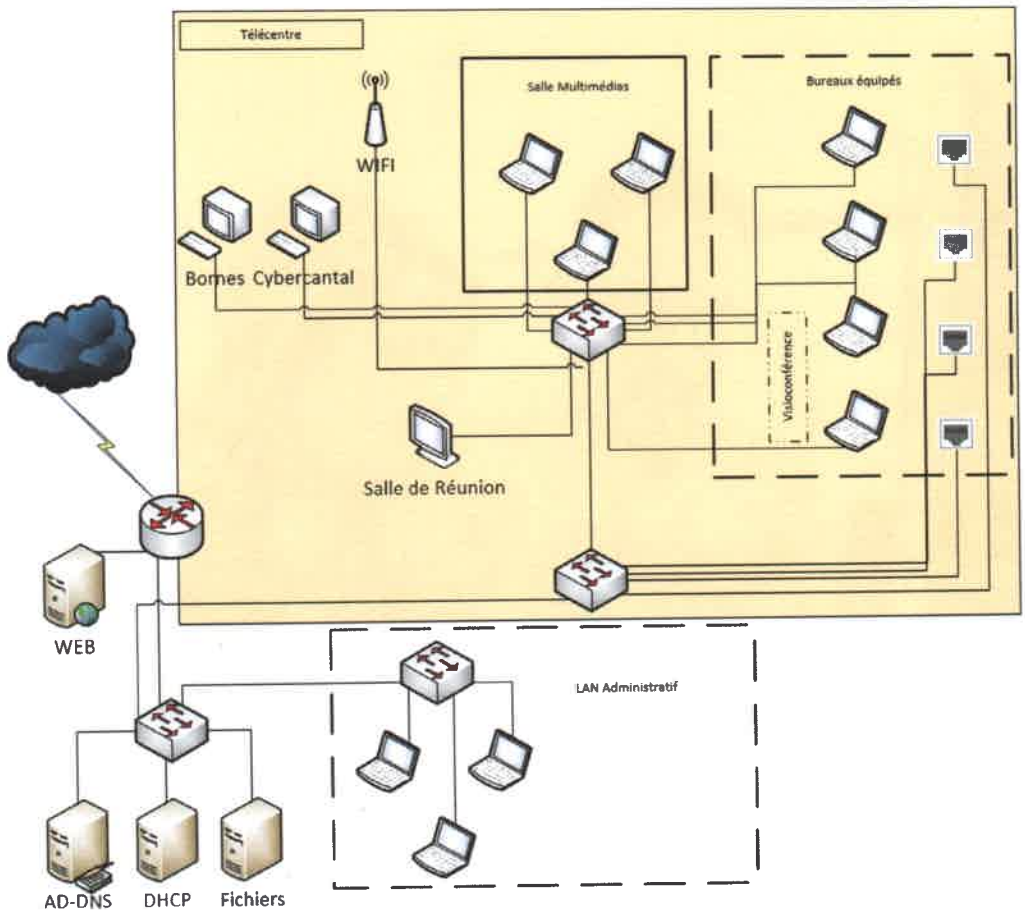
Le prestataire informatique

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 privilèges 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.