BTS SIO Services Informatiques aux Organisations	Module **B3** Cybersécurité des services informatiques
Seconde année	**Cours ou Travaux Pratiques**
SLAM Solutions logicielles et applications métier	**SIO2-SLAM-B3-REVISION-TD-02**

SIO2-SLAM-B3-REVISION-TD-02

THÈME 1 : Protéger les données à caractère personnel

LE CONTEXTE

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

Mme 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 Mme Chevance, vous devez vérifier si l'enterprise 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 ci-dessous.

QUESTIONS

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

Mme Chevance s'interroge sur la responsable 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

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

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

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.

• 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

FICHE SAVOIR CEJM APPLIQUÉE 3

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

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 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.

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 SAVOIR 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.

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.

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.

Les moyens de la preuve électronique

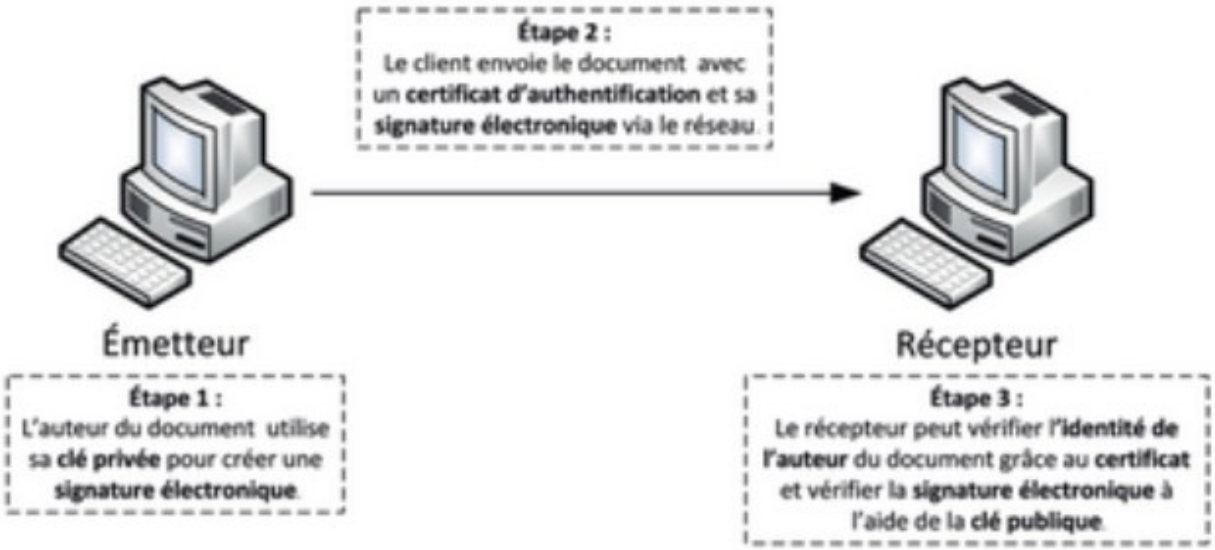
1. Les moyens/supports de l'authentification

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».