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

WEB

www.tienmini.fr/6988/2001

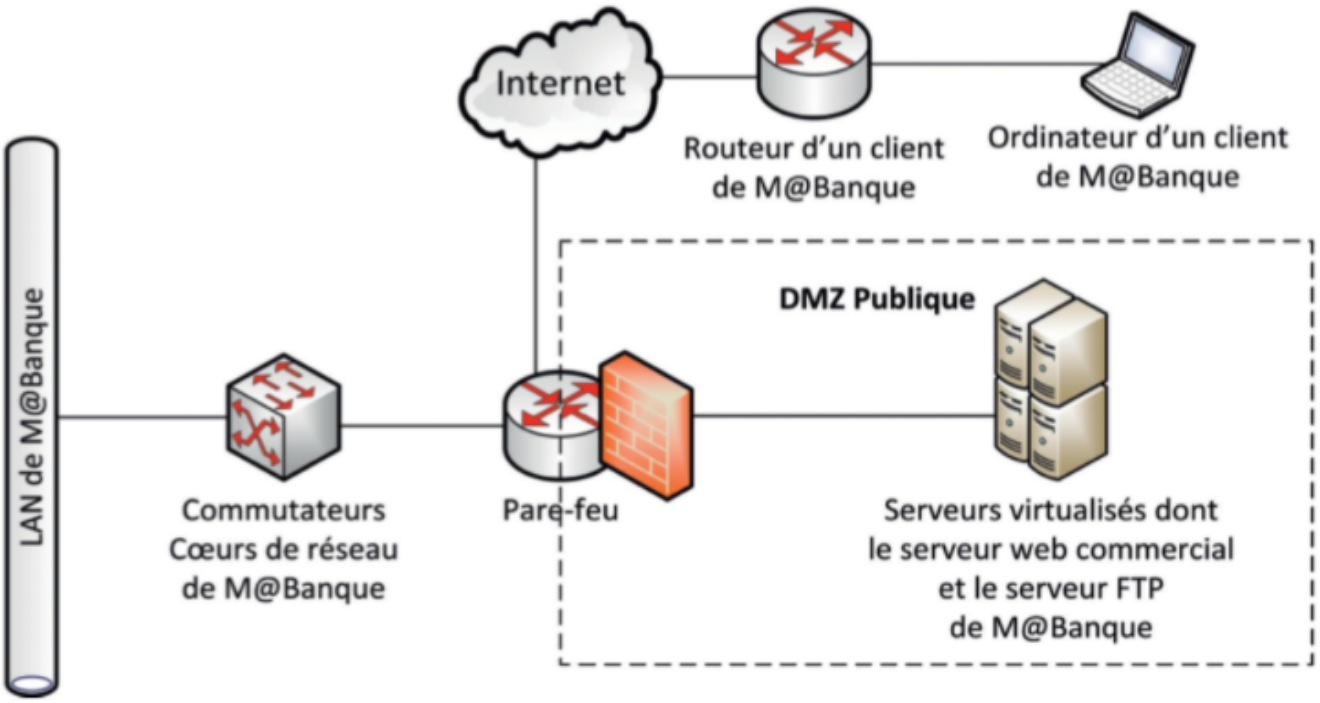
Le prestataire informatique

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.

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

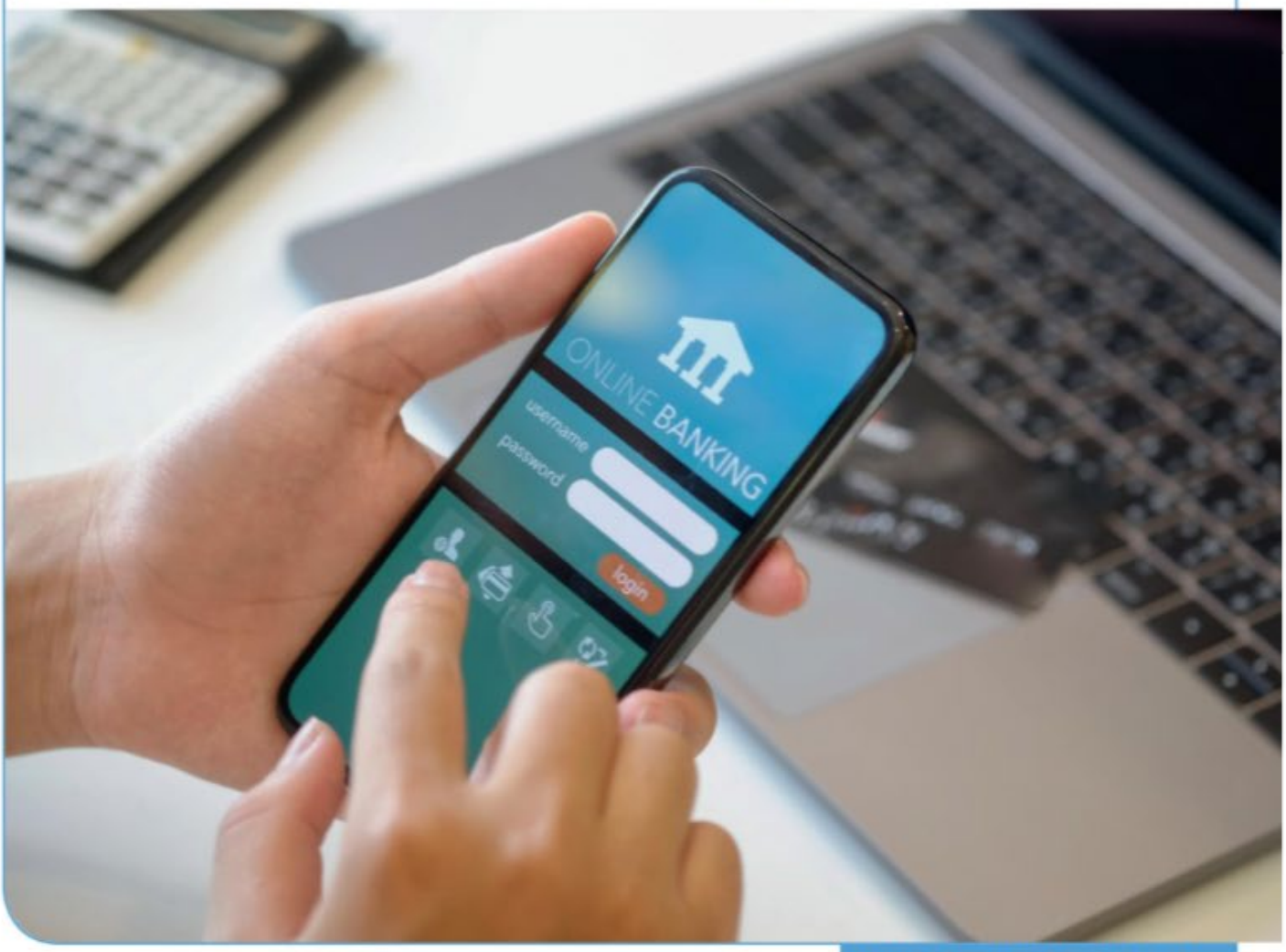
- L'identité numérique de l'organisation : risques et protection juridique
- Droit de la preuve électronique
- Les risques des cyberattaques pour l'organisation : économique, juridique, atteinte à l'identité de l'entreprise

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 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

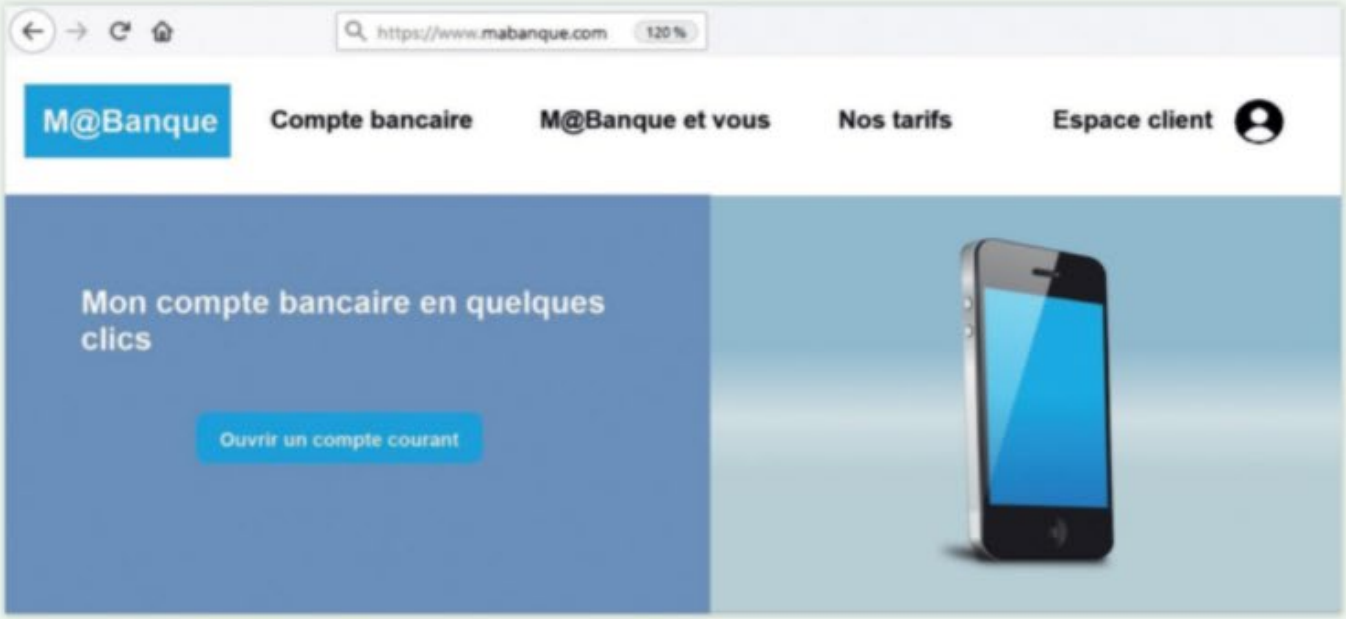
   Les hackers du site de M@Banque ne se sont pas contentés de commettre cet acte de malveillance. Ils ont également diffusé de mauvaises appréciations sur les réseaux sociaux, ce qui a amené de nombreux clients à envoyer des courriels pour exprimer leurs inquiétudes.
5. Rédigez une note à l'attention de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

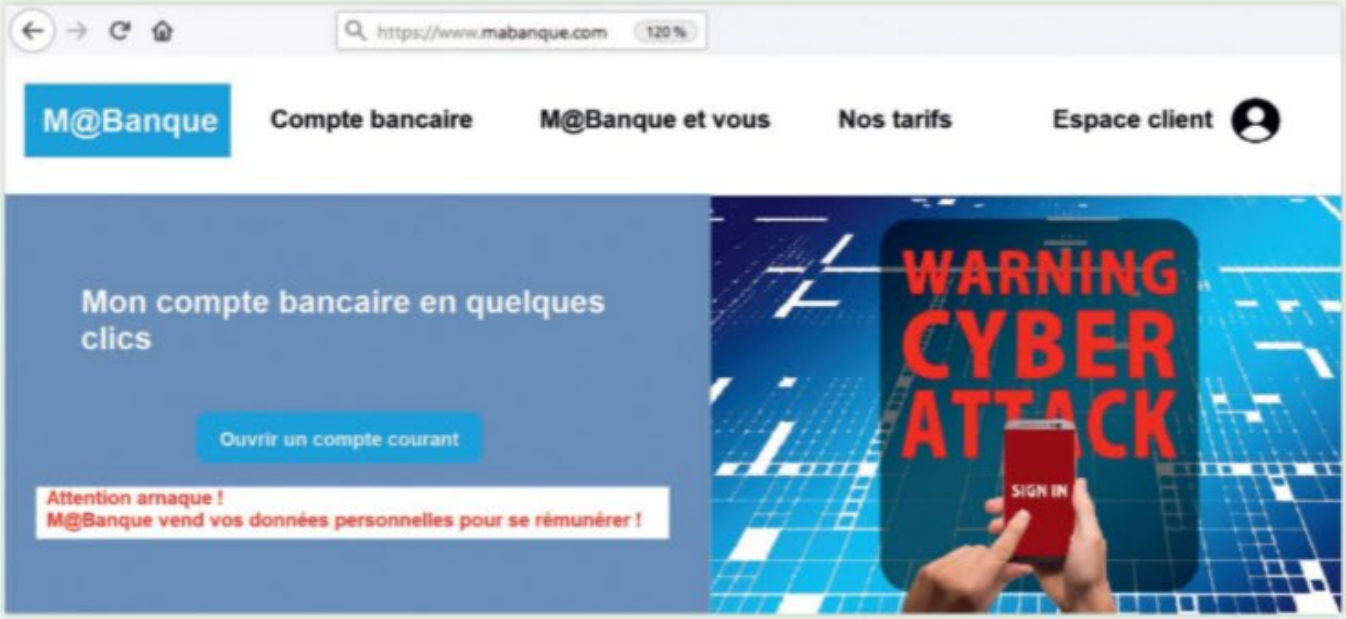
Dossier documentaire

Document 1 Le site défiguré de M@Banque

L'apparence du site avant sa défiguration



L'apparence du site après sa défiguration

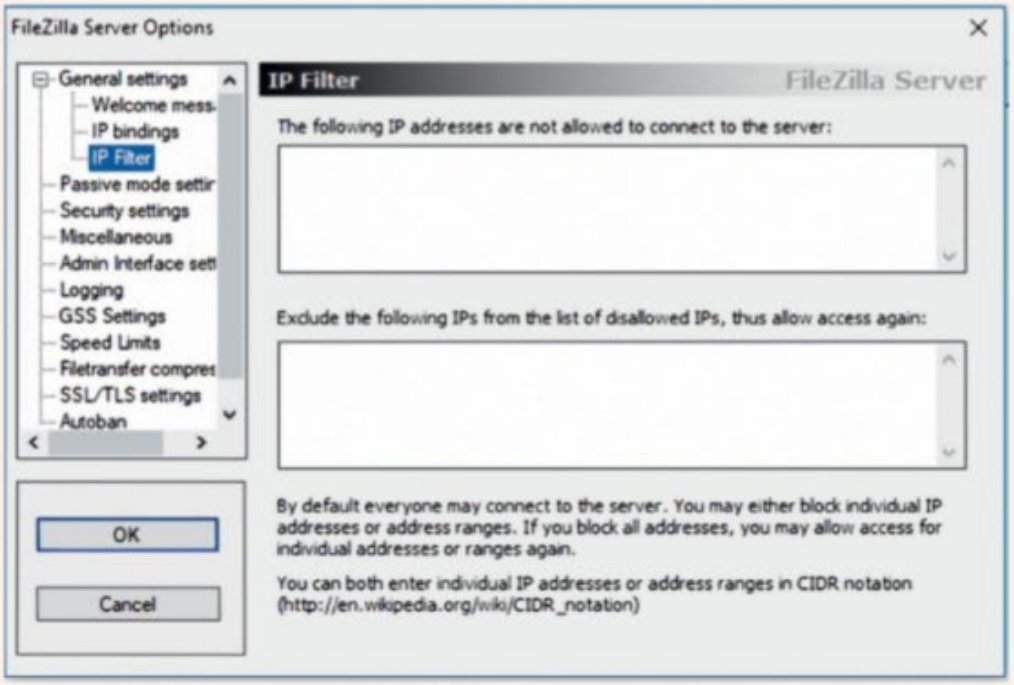


Document 2 Extrait du fichier *log* du serveur FTP

```
(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@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.

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 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
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 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