Chapitre 3
Préserver l'identité numérique
De l'organisation

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

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

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

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

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

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

L'incrimination principale qui peut être retenue ici est celle de l'entrave à un système de traitement automatisé de données (STAD ou système d'information). Les articles 323-1 à 323-7 du Code pénal disposent :
- le fait d'accéder ou de se maintenir, frauduleusement dans un système de traitement automatisé de données (par exemple en utilisant le mot de passe d'un tiers ou en exploitant sciemment une faille de sécurité) ;
- le fait d'introduire frauduleusement des données dans un système de traitement automatisé de données. Ce texte peut s'appliquer dans le cadre de la défiguration de site. La défiguration désigne la modification non sollicitée de la présentation d'un site web, à la suite d'un piratage du site ;
- le fait d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données d'un système de traitement automatisé de données. La copie

frauduleuse de données (souvent improprement qualifiée de « vol » de données) pourra être donc sanctionnée sur ce fondement ;
- le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données ;
- les tentatives de ces infractions sont punies des mêmes peines.

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

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

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

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

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

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

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

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

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