GAGNE Mattéo
AKILABANA Joseph
BTS SIO-1
Bloc 3 - Cybersécurité

TD-3 : Identité Numérique M@Banque

23/11/2024

1°) Site de M@Banque avant défiguration

Il y a plusieurs élément se rapportant à l'identité numérique de M@Banque :

Le logo de M@Banque(2) ; Le nom de domaine du site (1) ;
La plate-forme du site pour se créer un compte bancaire en quelques clics (7) ;
Plusieurs rubriques sont mises en place par exemple : Compte bancaire (3) ;
M@Banque et vous (4) ;Nos tarifs (5) ;Et l'Espace client (6).

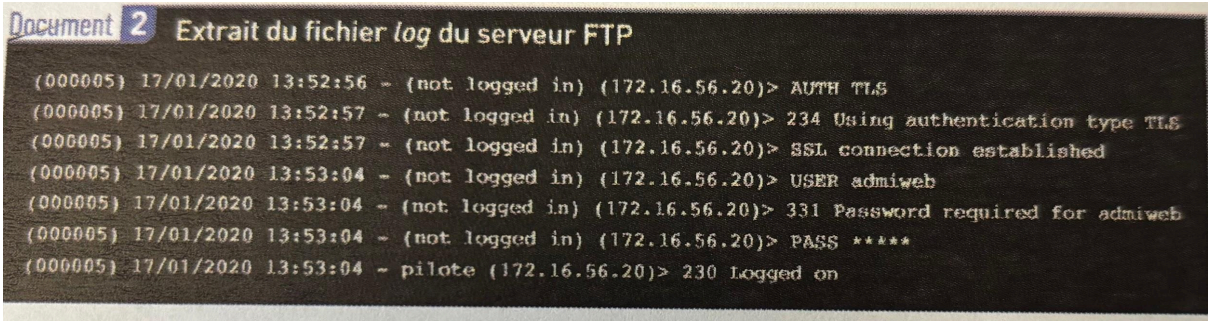
2°) Risques économiques et juridiques pour M@Banque

La perte de confiance des clients entraîne en effet une violation de données pouvant gravement nuire à la e-réputation de M@Banque, poussant les clients à rechercher une néo banque plus sûre.

La perte de confiance ce suit avec une baisse du chiffre d'affaires.
Les clients victime de fraude peuvent demander une indemnité ou un remboursement suite à ça.
Il peut y avoir des poursuites en justice pour non-conformité des données qui ne respectent pas la réglementation au sécurite par exemple: RGPD.

Il y a des sanctions financières et ils vont restreindre les activités de M@Banque dans certains domaines.

3°) Journal d’activités du serveur FTP


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
```

Le serveur FTP est configuré pour utiliser une authentification TLS, ce qui est une bonne pratique en termes de sécurité.
Le protocole TLS ne suffit pas à lui seul à assurer la sécurité des e-mails, car il ne protège que contre certaines formes d'attaques par e-mail. Le protocole TLS est particulièrement efficace contre les attaques de type « man-in-the-middle » et les attaques par écoute clandestine, qui se produisent pendant le transit des données.

Cependant, certaines vulnérabilités potentielles peuvent exister :

- Politique de mot de passe :

Si le mot de passe utilisé est faible ou commun à plusieurs personnes, il pourrait représenter une vulnérabilité, il faudrait donc s’assurer que les mots de passe utilisés soient forts, complexes et changer / régénérer régulièrement.

- Tentatives de connexion :

Le fichier montre plusieurs tentatives de connexion non authentifiées, il serait donc préjudiciable de surveiller et de limiter les tentatives de connexion échouées pour prévenir les attaques de force brute.

- Usage de l’authentification TLS :

Bien que TLS soit sécurisé, il est essentiel de vérifier que les versions de TLS utilisées ne présentent pas de vulnérabilités connues ou ne soient obsolètes et donc s’assurer de maintenir le serveur à jour avec les derniers correctifs de sécurité.

4°) Solution technique pour remettre un site en bon état

Il est recommandé de mettre en place une politique de gestion des autorisations d’accès en passant par une liste blanche réduite d’adresses IP, depuis lesquelles des administrateurs ou des contributeurs peuvent légitimement effectuer des modifications.

Dans le cas où les adresses IP des administrateurs ne sont pas statiques, une authentification forte devra être envisagée (validation de certificats clients, par exemple).

Pour remettre le site de M@Banque en bon état de fonctionnement après sa défiguration, il est recommandé de désactiver le site web immédiatement pour éviter toute utilisation frauduleuse ou propagation de la défiguration ;

- Conserver les journaux du serveur en prenant des captures d'écran et d'autres preuves de l'attaque pour une analyse ultérieure et aider les autorités.

- Signaler l'incident aux autorités compétentes, telle que l'agence de cybersécurité nationale.

- Engager un expert en cybersécurité pour analyser l'attaque, identifier les failles de sécurité et comprendre comment les hackers ont accédé au site.

- Corriger les vulnérabilités identifiées par l'expert en cybersécurité, cela peut inclure la mise à jour des logiciels, la correction des configurations de sécurité et le renforcement des mots de passe.

- Restaurer le site à partir d'une sauvegarde précédente ou réparer les modifications apportées par les hackers.

- Mettre en place une surveillance continue des activités sur le site pour détecter toute activité suspecte ou nouvelle tentative d'attaque.

- Informer les utilisateurs du site de l'incident et des mesures prises pour sécuriser leurs données.

- Revoir et améliorer les politiques de sécurité de l'entreprise pour prévenir de futures attaques.

- S'assurer que le personnel est formé aux meilleures pratiques de cybersécurité pour éviter des incidents similaires à l'avenir.

5°) Note à l’attention de Mme Schmitt

Moyens de protection juridique pour protéger l’identité numérique de M@Banque.

Pour protéger l'identité numérique de M@Banque après l’attaque voici les élément à mettre en oeuvre:

Porté plainte contre diffamation du site M@Banque pour sanctionner les attaquants, et faire part du problème à la CNIL (Commission Nationale de l’informatique et des Libertés) le plus vite possible.

Renforcer la sécurité par le DPO (Délégué à la protection des données) pour éviter de nouveaux incidents, sensibiliser les ménages contre les attaques extérieures comme intérieures notamment par des gestes de sécurité.
Demander la suppression des contenus dénigrants ou de phishing liés à l’entreprise M@Banque.

Si M@Banque est assurée contre les cyberattaques, il est important d’informer l’assurance rapidement pour qu'ils puissent intervenir et couvrir les pertes éventuelles.
Signaler les violations de données personnelles aux autorités de protection des données et aux utilisateurs concernés dans un délai de 72 heures.

En plus des moyens juridiques, il est essentiel de renforcer les mesures de sécurité techniques pour prévenir de futures attaques.