Compte-rendu du TD3 du thème 2

Valentin Massat-Seiller et Micael Souza De Almeida

25/11/24

Mme Guelinel

Sommaire

I/ Analyse du site défiguré ainsi que les risques encourus (doc.1)

1. Les différents éléments de défiguration présents sur ce site sont:
   - Une première défiguration du site pour annoncer que M@banque vend les données des utilisateurs.
   - Deuxièmement, la modification de l'image d'un téléphone à droite de la page remplacer par une image où il est écrit "Warning cyber attaque"(Attention cyberattaque).

   Ces deux éléments sont donc liés à la défiguration du site et font ainsi perdre en crédibilité M@banque.

2. Comme dit précédemment M@banque risque tout d'abord une perte de crédibilité ce qui lui fera perdre une partie de son chiffre d'affaires ainsi que la confiance des clients. Et juridiquement, il y a deux risques:
   - Le premier serait que le ou les hacker(s) aient accès à des données compromettantes (en rapport avec les clients)
   - Ou, au contraire, que M@banque vend les données de ces utilisateurs et qui pourrait entraîner une enquête en leur défaveur.

II/ Analyse technique de la défiguration du site (doc.2,3,4)

3. La vulnérabilité dans le cas des documents relève du manque de filtre au niveau des adresses IP en donnant des autorisations de connexion en tant qu'admiweb à tout ce qui tente la connexion, ce qui entraîne la menace exploitée par l'attaquant. Et a ainsi pu défigurer le site. Les log du serveur FTP servent notamment à retracer l'adresse IP de l'attaquant et ainsi apporté une preuve concrète de l'attaque.

4. Une première mesure serait d'imposer une whitelist d'adresses IP pour que seule les adresses IP des admins puissent se connecter en tant que telle. Ou, comme dit dans le document 4, créer un mot-de-passe fort en cas de connexion des admins depuis un poste qui ne serait pas un des appareils de cette whitelist.
   Et deuxièmement, on peut retracer dans les logs les modifications du contenu du site pour, par la suite, écrire et utiliser les commandes inversant la défiguration du site.

III/ Ecriture d'une note de synthèse à l'attention de Mme Schmitt (doc.5)

Note à l'attention de Mme Schmitt

Objet : Protection juridique de l'identité numérique de M@Banque

Madame,

Suite à la défiguration du site de M@Banque et à la rumeur négative qui en découle, il est nécessaire de prendre des mesures juridiques pour limiter l'impact de ces événements sur l'image de l'entreprise. Le message suivant sur Twitter illustre les risques :

"M@Banque est à l'image de son site commercial. Aucune sécurité de nos données n'est garantie il faut tous fermer nos comptes avant que les pirates emportent notre argent !!!"

Voici les principales actions à envisager pour protéger l'identité numérique de M@Banque :

1. **Demande de retrait de contenu illicite** : En cas de messages diffamatoires, il est possible de demander leur retrait auprès des plateformes (comme Twitter) via l'article 6-I-5 de la LCEN.
2. **Action en diffamation** : Si les propos sont mensongers, une action en justice peut être envisagée pour préserver la réputation de l'entreprise.
3. **Veille numérique** : La mise en place d'une surveillance sur les réseaux sociaux permet de repérer et gérer rapidement les rumeurs ou accusations infondées.

4. **Communication de crise** : Répondre rapidement aux accusations avec des clarifications publiques, notamment concernant la sécurité des données, est essentiel.
5. **Renforcement de la cybersécurité** : Prendre des mesures immédiates pour sécuriser le site et rassurer les clients sur la protection de leurs données.

Ces actions permettront de limiter les préjudices juridiques et réputationnels.

Cordialement,
Valentin Massat-Seiller