BLOC 3

MOHAMED HAFAIDH KERVIN BERNARD	CyberSécurité	Date: 20/10/2023

M@Banque

Cybersécurité des systèmes

1. La différence entre les deux sites web est presque la même car le nom domaine et le même que sur le site piraté et nous pouvons pas avoir deux sites avec le même nom de domaine. Le site web de **M@Banque** c'est fait piraté directement pour leur faire passer pour un site Web pas officiel. Le changement a été réalisé sur la page de création de compte, avec une image de (Warning CYBERATTACK) puis avec un texte qui nous avertit << attention arnaque ! M@Banque vend vos données personnelles pour se rémunérer !>>

2. Les risques économiques et juridiques encourus par M@banque sont les vols de données personnelles et vols de page de création de compte les juridique peut être Profession libérale en nom propre est la forme juridique la plus fréquente pour les professionnels est la profession libérale indépendante. Cette activité libérale est souvent au nom du créateur.

3. En voi que dans les extrait du fichier log du serveur FTP que il y a quelqu'un qui c'est connecté à 17/01/2020,13:53:04 en vois que tout les information sont relevée sauf le mots de pass mais l'adress IP est relevée du coup si vous travailler dans l'entreprise vous pouvez: Déjà filtrer les Adress IP qui sont sont pas autorisés dans le serveur et vous pouvez exclure les IP suivant du IP non autorisée d'avant et rendre accés encore

4. La limitation de l'accès à l'interface de gestion est essentielle à la sécurité d'un site web. Si vous pensez qu'il y a une fraude, voici quelques étapes rapides que vous pouvez suivre :

Isoler le site : Mettez immédiatement le site en mode maintenance ou hors ligne pour éviter tout accès non autorisé pendant que vous enquêtez sur l'incident. Vous pouvez généralement le faire en renommant temporairement le fichier d'index du site

(index.php, index.html, etc.) ou en utilisant un plugin de maintenance si vous utilisez un système de gestion de contenu (CMS) comme WordPress.

Vérifier les journaux d'accès : Consultez les journaux d'accès du serveur web pour identifier l'adresse IP ou les adresses IP à partir desquelles l'accès non autorisé a été tenté. Cela vous aidera à comprendre l'étendue de l'incident.

Révoquer les droits d'accès non autorisés : Si vous avez identifié des adresses IP suspectes, bloquez-les immédiatement à l'aide de votre pare-feu ou de vos règles de sécurité réseau. Assurez-vous que seules les adresses IP approuvées ont accès à l'interface d'administration.

Changer les identifiants d'administration : Modifiez les mots de passe et les identifiants d'accès à l'interface de gestion. Assurez-vous d'utiliser des mots de passe forts et différents pour chaque compte.

Analyser le site pour les failles de sécurité : Procédez à un audit de sécurité pour identifier et corriger toute vulnérabilité sur le site web qui a pu être exploitée par l'attaquant. Cela peut inclure des mises à jour de logiciels, des correctifs de sécurité, etc.

Restaurer le site depuis une sauvegarde fiable : Si le site a été compromis, restaurez-le à partir d'une sauvegarde antérieure à l'incident. Assurez-vous que la sauvegarde est propre et n'a pas été altérée.

Examiner le code malveillant : Si du code malveillant a été injecté sur le site, recherchez et supprimez-le. Vous devrez peut-être demander l'aide d'un professionnel en sécurité informatique pour cette étape.

Surveiller les activités : Mettez en place une surveillance continue pour détecter toute activité suspecte sur le site. Les solutions de détection d'intrusion peuvent être utiles pour cette tâche.

Mettre à jour la politique de gestion des autorisations : Revoir et renforcer la politique de gestion des autorisations d'accès, en suivant les recommandations du CERT-FR. Mettez en place des listes blanches d'adresses IP autorisées et envisagez des mesures d'authentification forte si nécessaire.

5 :

Madame Schmitt,

En référence au message sur le compte Twitter de M@Banque publié par @ClientMécontent, je tiens à souligner que les propos tenus dans ce tweet sont diffamatoires et préjudiciables pour notre entreprise. Pour contrer de

telles attaques à notre réputation en ligne, nous pouvons envisager d'utiliser les moyens de protection juridique mentionnés précédemment.

Ce tweet porte atteinte à la réputation de M@Banque en suggérant que la sécurité des données de nos clients est compromise, ce qui peut dissuader d'autres clients potentiels de faire affaire avec nous. Par conséquent, nous pourrions envisager les étapes suivantes pour protéger notre identité numérique :

1. Signaler le Tweet : Vous pouvez signaler ce tweet à Twitter en utilisant l'option de signalement de contenu diffamatoire ou nuisible. Twitter peut prendre des mesures pour le retirer s'il viole leurs règles d'utilisation.

2. Contacter un Avocat : Il serait judicieux de consulter un avocat spécialisé en droit de l'internet pour évaluer si des actions en justice pour diffamation peuvent être engagées contre l'auteur du tweet. Ce professionnel pourra vous conseiller sur les étapes à suivre.

3. Répondre au Tweet : Dans le respect des lois sur le droit de la presse, M@Banque peut envisager de répondre publiquement à ce tweet pour rectifier les informations erronées et rétablir la vérité. Il est important de rester professionnel et de ne pas entrer dans des conflits en ligne.

4. Surveillance Continue : Assurez-vous de surveiller de près les médias sociaux et de signaler rapidement tout contenu diffamatoire ou préjudiciable. Une action rapide peut contribuer à minimiser les dégâts potentiels.

5. Sensibilisation à la Sécurité des Données : Profitez de cette opportunité pour informer nos clients des mesures de sécurité en place et de notre engagement envers la protection de leurs données.

Je vous encourage vivement à prendre des mesures immédiates pour faire face à cette situation et à consulter un avocat pour évaluer les options légales à votre disposition. La protection de notre identité numérique est essentielle pour maintenir la confiance de nos clients.

N'hésitez pas à me contacter si vous avez besoin d'assistance supplémentaire ou de recommandations spécifiques pour agir dans cette situation.

Cordialement,