Zohir Tamda
SIO1 groupe 2
Bloc 3 - Cybersécurité

Le 6 novembre 2023

Protéger l'identité numérique de l'organisation

Sommaire

Eléments

L’identité numérique est l’ensemble des traces numériques qu’une personne ou une collectivité laisse sur le réseau Internet. Sur la défiguration, nous remarquons une alerte disant ‘Attention arnaque’ ainsi que l’image d’origine à changer, en plus du logo “warning cyber attack”.

Cependant l’apparence du site reste la même avec le même nom de la banque, la même barre de menu, le même lien internet et les mêmes fonctionnalités en générale.

Risques économiques et juridiques

La défiguration d'un site web consiste au piratage de l’apparence du site Internet d’une entreprise. Certaines modifications telles que le changement d’une image, un texte, l’insertion d’une vidéo, l’insertion d’un audio sont dans le but de changer l’apparence.

Le but étant de démontrer un certain contrôle du site. Les risques encourus ainsi que les préjudices sont nombreux, concernant l’organisation : perte de confiance des clients, conséquences du non-respect du règlement général sur la protection des données.

Les risques juridiques plus conséquents sont 60 000€ d’amende 300 000€ et de 2 à 7 ans de prison. Pour les utilisateurs de la banque, les risques : l’indisponibilité du site Internet, accessibilités aux données des utilisateurs.

Vulnérabilité

Le protocole FTP (File Transfer Protocol) permet d'échanger des fichiers/dossiers entre le client et le serveur. Le serveur FTP possède une couche de sécurité qui permet de crypter les informations lors des échanges: c'est le SSL/TLS (Secure Sockets Layer/Transport Layer Security).

Cependant, le mot de passe de l'utilisateur 'admiweb' n'est pas robuste: il comporte 5 caractères. Également, l'accès au serveur FTP n'est pas configuré. Les filtres IP ne sont pas définis par défaut, ce qui fait que n'importe qui peut accéder à ce serveur s'il possède le nom d'utilisateur et le mot de passe, ou bien qu'une personne mal intentionnée peut accéder au serveur en utilisant l'attaque par force brute. Ce qui démontre ses vulnérabilités.

Les solutions techniques

Pour pallier ces problèmes, plusieurs solutions sont possibles : envoyer un message par téléphone ou par mail que notre site M@Banque a subi une défiguration.

Et nous allons procéder à un renouvellement immédiat du site et du serveur :

- Débrancher le câble du serveur et il faudra néanmoins conserver des preuves de cet actes frauduleux grâce au fichier log.
- Corriger en permanence les failles informatiques.
- Utiliser un protocole sécurisé, tels que le protocole SFTP (Secure File Transfer Protocol) ou SSH (Secure Shell).
- Porter plainte et se mettre en relation avec la justice rapidement.

Les moyens de protections juridiques

Bonjour Madame Schmitt,

La e-réputation de votre banque sur les réseaux sociaux a été fortement atteinte, les acteurs malveillants publient en ligne des commentaires mécontents. Ils veulent montrer que la sécurité numérique de la banque n’est pas sécurisée.

La sécurité informatique est indispensable, quel que soit le type de réseau qu’on utilise. Cependant, le serveur web que vous avez en possession pour permettre de publier votre site web présente des failles de sécurité, notamment l'authenticité. Ce qui a pour conséquence de nuire à l'activité de votre banque.

Voici les procédures à respecter pour améliorer la sécurité informatique:

Il est recommandé d’utiliser un mot de passe avec des caractères aléatoires, ce qui permet de rendre le mot de passe plus sécurisé.

Il est également indispensable de configurer les filtres IP pour empêcher les utilisateurs hormis le développeur web de pouvoir accéder au serveur, ce qui garantit sa sécurité.

Enfin, agir en chiffrant les données et en communiquant sans l'information de son identité et tout simplement en utilisant des adresses IP anonymes.

En respectant ces moyens de protection, vous améliorez l'authenticité de votre serveur web et ainsi faire face aux vulnérabilités.

En résumé, restez vigilant et méfiant, évitez de faire confiance trop rapidement. De plus, améliorez l'authenticité de votre serveur web pour renforcer votre protection contre les menaces informatiques.

En espérant avoir répondu à vos problématiques, Madame Schmitt, mes très sincères salutations.

Webographie

https://www.generali.fr/entreprise/actu/proteger-reputation-image-entreprise/

https://www.cairn.info/revue-questions-de-management-2019-1-page-53.htm

https://www.guest-suite.com/blog/protection-e-reputation

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/defiguration-de-site-internet

https://www.ihemi.fr/formations/ressources-pedagogiques/kit-de-sensibilisation/les-risques-informatiques-la-defiguration-de-site