ESTEVES Lola BALDA Nilda SIO 1 G1	Le 20/10/2023

Bloc 3 - Cybersécurité

Thème 2: Protéger l'identité numérique de l'organisation

Sommaire

1. les éléments se rapportants à l'identité numérique de M@Banque :

Sur l’identité numérique de la banque, il y’a des différentes éléments comme : le nom de la banque, le logo de la banque, les tarifs, et une espace “Ma banque et vous” il s’agit d’un lieu d'échange fictif ou on peut retrouver les coordonnées de la banque, par exemple le numéro de téléphone, l’adresse mail.
Sur le site défiguré l’image d'accueil de l’entreprise à changer en sorte qu’elle dénonce l’entreprise de vol de données.

2. Les risques économique et juridique

Les risques juridique :

Si la violation entraîne un risque pour les droits et libertés des personnes concernées, le responsable du traitement doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ; doit notifier cette violation à la CNIL, au plus tôt et dans un délai maximum de 72h.

Les risques économiques:

Sont la perte d’argent et de de données des clients qui les clients eux aussi peuvent perdre leur argent.Et l'accès à leur compte si les attaquants a pour but de connaître également le mot de passe .une personne non identifiée se connecte en tant qu’administrateur.

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

On peut constater sur le document 3 qu'il on mis aucun filtre et que tout le monde peut y accéder .Il faut donc configurer l'adresse ip ce qui est une vulnérabilité.L'attaquant utilise la méthode d'attaque suivante : L'attaque beast.

On peut constater sur le document 2 :
Il utilise un protocole tls qui est vulnérable car ce n'est pas assez sécurisé car la clé de déchiffrement est pareil que celle du chiffrement donc si l'attaquant connaît la clé du chiffrement il connaît aussi la clé de déchiffrement

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

Une solution technique à cet acte frauduleux, c'est d'utiliser une version plus récente et plus sécurisé du SSL ou TLS, elle permet tout simplement à une personne malveillante de déchiffrer le contenu d'une session chiffrée à l'aide de SSL ou TLS entre un navigateur et un site Web. Et voici une démarche pour remettre le site en bon état de fonctionnement, définir les adresses ip qui peuvent se connecter et exclure les autres définir des black liste et des whitelist on peut aussi mettre en place une politique de gestion de données .

5.Rédiger 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 faites attention au information de votre entreprise que vous mettez sur votre site par exemple les trace que vous laissez sur internet comme les commentaire les avis qui resteront à tout jamais sur internet .Pour les moyens juridique pour protéger votre identité numériques est la suivante :pgp qui repose sur une cryptographie de clé publique .


CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -
CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -

fin