TP Identité Numérique

Contexte

M@Banque est une néobanque fondée en 2018 sur le modèle de banques en ligne comme Orange Bank, N26 ou Revolut, les leaders actuels du marché. Moins chère que les banques physiques, une néobanque offre des services plus restreints mais ciblés, tels que l'ouverture sans délai d'un compte courant, ou encore des outils innovants de gestion des transaction financières (retrait, virement, dépôt), exclusivement sur l'application mobile. La législation a favorisé l'essor des néobanques en obligeant les banques à faciliter la mobilité bancaire. Leur activité purement digitale les amène à porter une attention toute particulière à la protection de leur identité numérique.

Table des matières

1) Défiguration et identité numérique

Repérez, sur le site défiguré, les éléments se rapportant à l'identité numérique de M@Banque.

Tous les éléments entourés en rouge permettent d'identifier l'identité numérique de M@Banque.

2) Risques économiques et juridiques

Identifiez les risques économiques et juridiques encourus par M@Banque suite à la défiguration de son site et à l'accès à des données personnelles de ses clients.

Les risques économiques encourus sont : une perte de client potentiel suite à une incertaine sécurité mise en place qui peut effrayer. Les actions en bourse si présente vont-elles aussi chutés. La défiguration sur le site internet entraîne une perte économiques importante pour l'entreprise.

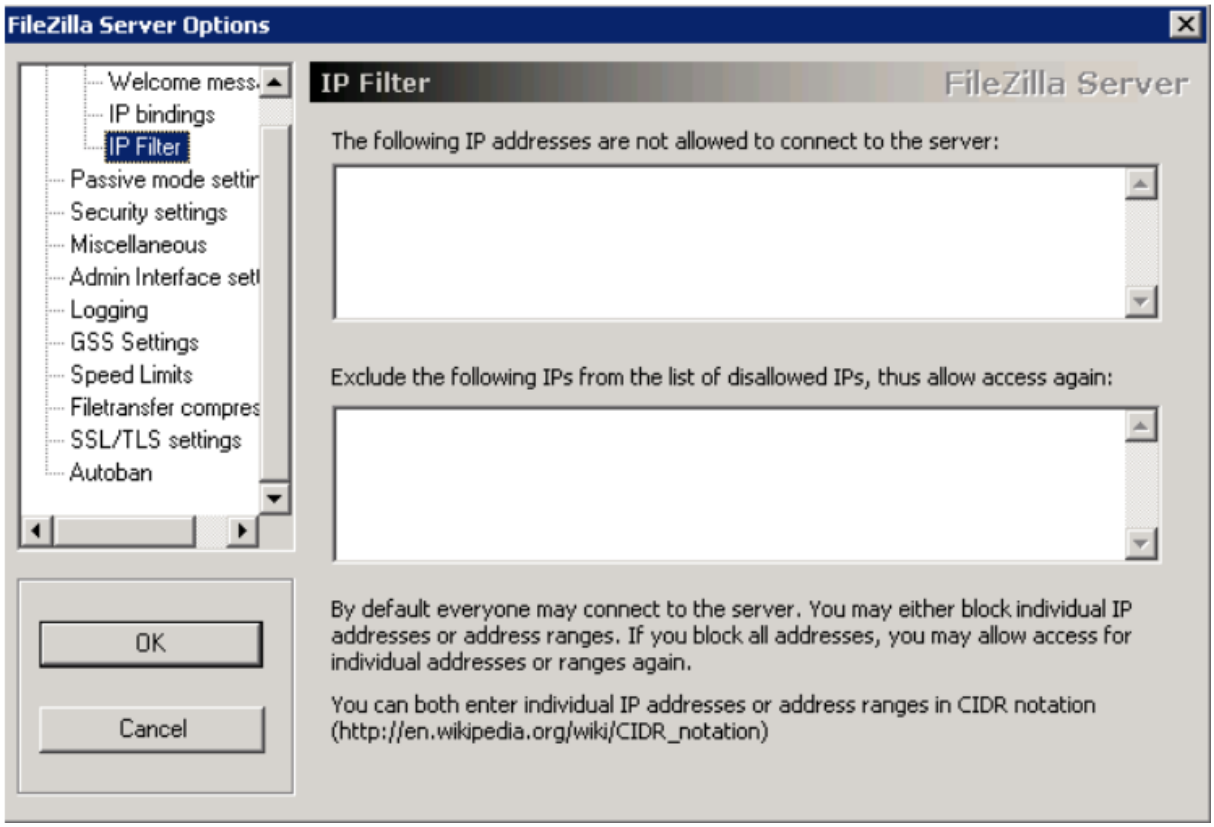
Les risques juridiques qui en suivent sont les suivants : Si le site internet gère des données personnels, l'entreprise est responsable de garder intègre les donnes personnelles de leur client. De ce fait elle encoure des peines pénales en cas de non-respect de cette règle.

3) Vulnérabilité FTP

Les pages du site commercial de M@Banque sont régulièrement mises à jour par un seul développeur, uniquement depuis son poste de travail dédié (adresse IP : 172.16.8.10/16). Il utilise le logiciel Filezilla (côté client et côté serveur) afin de transférer les fichiers en FTP. Voici les traces (« logs » ou « journaux d'évènements ») laissées par l'attaquant :

```
(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
```

Configuration du filtrage d'adresse IP au niveau du serveur FTP :



Identifiez la vulnérabilité et le scénario d'attaque en vous aidant de ces différentes informations. Quels sont les critères de sécurité défaillant ?

La vulnérabilité principale dans ce scénario est l'utilisation d'un protocole de transfert de fichiers non sécurisé, FTP (File Transfer Protocol). FTP n'utilise pas de chiffrement pour protéger les données transmises, ce qui signifie que les informations sensibles, telles que les informations de connexion et les données confidentielles, peuvent être interceptées et lues par des tiers malveillants.

Un scénario d'attaque possible serait un pirate informatique qui utilise des outils pour scanner les ports ouverts sur l'adresse IP spécifiée (172.16.8.10/16), dans l'espoir de découvrir une connexion

FTP active. Une fois connecté, il pourrait utiliser des informations d'identification volées ou des techniques de force brute pour accéder aux fichiers sur le serveur et y apporter des modifications malveillantes, comme l'ajout de scripts malveillants.

Les critères de sécurité défaillants dans ce scénario sont l'utilisation d'un protocole de transfert de fichiers non sécurisé, l'absence de cryptage pour protéger les données transmises, et l'utilisation d'un seul développeur pour mettre à jour les pages du site, ce qui augmente les risques d'erreurs et de compromissions. Il serait conseillé de mettre en place une solution de sécurité pour protéger les données sensibles et utiliser des protocoles de transfert de fichiers sécurisés (comme SFTP ou HTTPS) pour garantir la confidentialité et l'intégrité des données. Il est également recommandé d'utiliser des méthodes d'authentification renforcées, comme l'utilisation de certificats SSL/TLS pour authentifier les utilisateurs et les serveurs, et de limiter l'accès à un groupe restreint d'utilisateurs ayant besoin d'accéder aux pages du site.

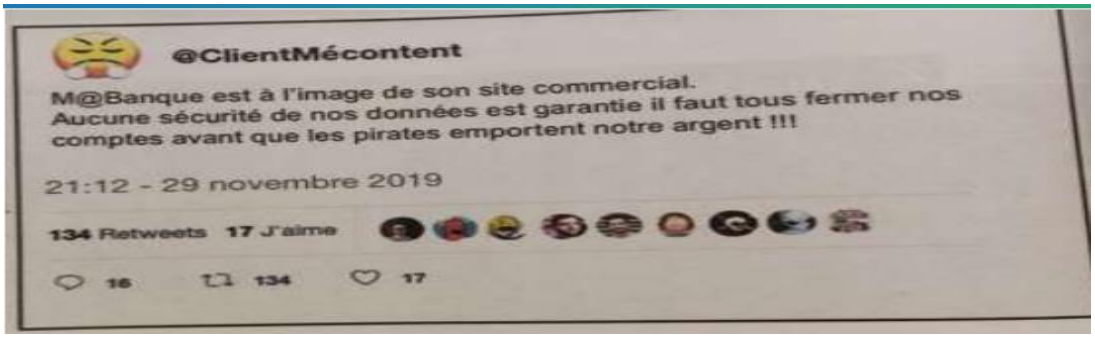
4) Remédiation

Proposez une solution technique pour éviter qu'une telle attaque se reproduise à nouveau et recommandez une démarche pour remettre le site en bon état de fonctionnement.

Il serait conseillé de mettre en place une solution de sécurité pour protéger les données sensibles et utiliser des protocoles de transfert de fichiers sécurisés (comme SFTP ou HTTPS) pour garantir la confidentialité et l'intégrité des données. Il est également recommandé d'utiliser des méthodes d'authentification renforcées, comme l'utilisation de certificats SSL/TLS pour authentifier les utilisateurs et les serveurs, et de limiter l'accès à un groupe restreint d'utilisateurs ayant besoin d'accéder aux pages du site.

5) Juridique

Suite à la cyberattaque, il y a eu un « bad buzz » sur les réseaux sociaux qui peut être préjudiciable pour l'entreprise comme le montre cette capture d'écran :



Rédigez 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.

Chère Madame Schmitt,

Je vous écris pour vous informer des mesures de protection juridique qui peuvent être mises en place pour protéger l'identité numérique de M@Banque suite à la cyberattaque récente.

Il est important de signaler immédiatement toute activité malveillante ou tout contenu illicite à un organisme de réglementation compétent (la Loi d'Orientation et de Programmation pour la Performance de la Sécurité Information (LOPPSI)). Cela permettra de prendre les mesures appropriées pour enquêter sur l'incident et de protéger les données de nos clients. Il nous faut récupérer des preuves électroniques, il est primordial de prouver que les fait ont été causé par une personne malveillante. Une signature électronique qui permet d'identifier le malfaiteur est indispensable.

Il est également recommandé de surveiller les réseaux sociaux et les forums pour identifier tout contenu diffamatoire ou toute information erronée qui pourrait causer des dommages à la réputation de l'entreprise. Si nécessaire, il est possible de demander la suppression de ce contenu en utilisant les procédures de notification de contenu illicite ou en prenant des mesures juridiques pour faire valoir nos droits à la réputation.

Il est important de mettre en place des politiques de sécurité solides et de sensibiliser les employés à la sécurité informatique pour minimiser les risques de futurs incidents. Il est également important de tenir les clients informés de tout incident de sécurité et de leur fournir des conseils sur la façon de protéger leurs propres données.

Enfin, il est recommandé de s'assurer que les contrats avec les prestataires de services et les partenaires commerciaux contiennent des clauses de protection de la confidentialité et de la sécurité des données pour minimiser les risques de fuites de données.