

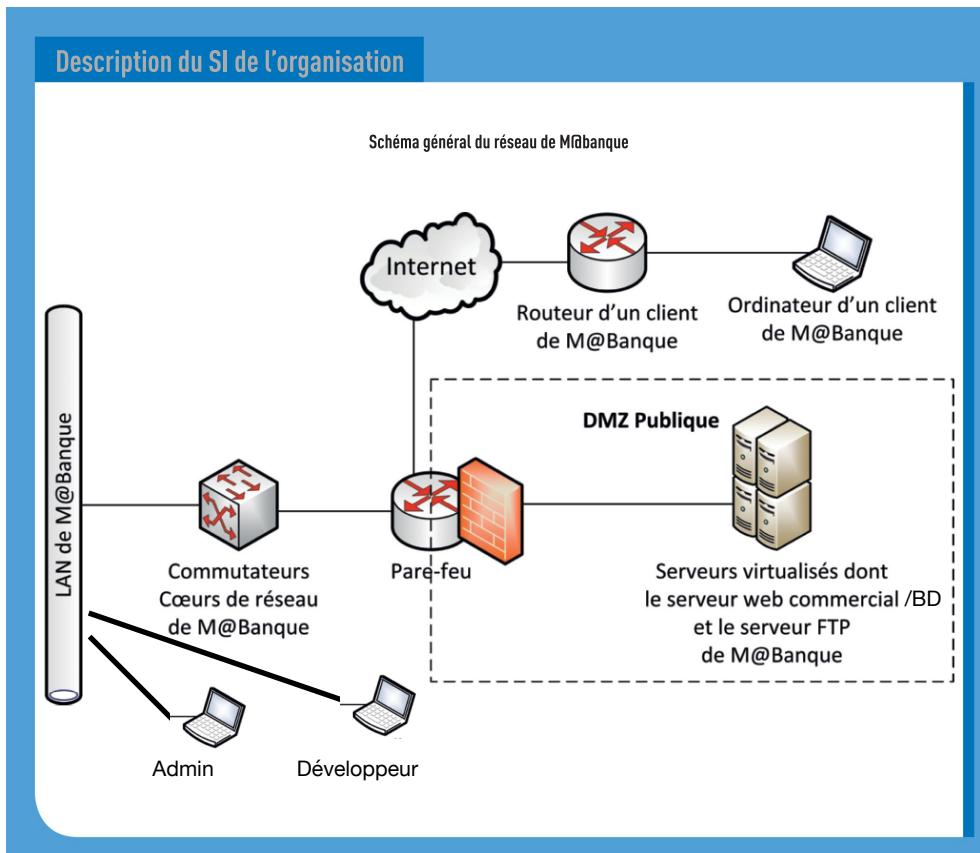
# Intégration des compétences

## Implémenter et sécuriser le cas M@Banque

### Objectif

Dans cet AP vous avez comme mission d'implémenter l'étude de cas M@Banque se trouvant dans votre livre de CyberSécurité (ch3, page 56), tout en intégrant les solutions techniques pour protéger cette banque des attaques la menaçant.

Vous travaillerez en binôme SLAM/SISR et vous utiliserez vos VM (Windows et/ou Linux selon votre choix) qui se trouvent dans la ferme serveur pour réaliser cet AP. Vous aurez donc une VM (ou plusieurs) pour mettre en place les serveurs demandés et une autre VM client pour jouer le rôle admin et développeur.



### Cahier des charges

La banque dispose :

- d'un serveur Web pour héberger son site qui permet aux clients d'accéder à leur espace bancaire : au minimum il faut une page d'accueil et une page d'authentification pour les comptes clients.
- d'une base de données pour gérer les comptes clients.
- d'un serveur AD pour gérer les sessions des employés (Il y aura donc au moins un compte développeur et un admin).
- d'un serveur FTP qui permet au développeur de mettre à jour le site web.
- d'un accès distant en SSH pour administrer les serveurs.
- d'un service de messagerie entre les clients et les conseillers : il faut créer au moins un compte mail client et un compte conseiller.

Comme indiqué dans votre livre, la banque a fait face à deux attaques (voir annexe)

- **Défiguration de son site web** : d'après les traces de log on remarque que l'attaquant a pu s'authentifier au serveur FTPS à cause du mot de passe faible. En plus, d'après l'interface de configuration du serveur FTP le paramétrage par défaut permet à n'importe qui de se connecter au serveur.
- **Hameçonnage** : des emails frauduleux ont été envoyés aux clients de la banque afin de voler leur identifiant/mot de passe et accéder à leur compte bancaire. La banque doit alors mettre en place une messagerie sécurisée pour éviter ce genre d'attaques.

### Solutions pour sécuriser les services de la banque

Pour sécuriser les services de la banque :

- Le serveur web doit être en **HTTPS**
- Au niveau du serveur de fichiers il est demandé :
  - d'utiliser **FTPS**
  - de désactiver les accès anonymes sur les services FTP en établissant une **liste blanche** : seul le développeur a le droit d'y accéder.
- Pour le site web : d'effectuer des **sauvegardes** régulières des données hébergées afin de faire face aux attaques de type défiguration ou rançomware : c'est à vous de mettre en place une stratégie de sauvegarde.
- d'utiliser une **politique de mots de passe** robuste pour les accès aux services.
- de mettre en place une **messagerie sécurisée** basée sur le chiffrement et la signature numérique pour garantir l'authentification et l'intégrité des documents échangés.

## Annexe

Document 1 Le site défiguré de M@Banque

L'apparence du site avant sa défiguration

L'apparence du site après sa défiguration

Attention arnaque !  
M@Banque vend vos données personnelles pour se rémunérer !

Document 1 Le courriel reçu par les clients de M@Banque

M@Banque

Cher(e)s clients et clientes de M@Banque

Vous trouverez en pièce-jointe le contrat d'ouverture de compte bancaire à compléter et à nous renvoyer pour confirmer votre engagement pris via notre site.

Vous devrez nous confirmer notamment votre identifiant et votre mot de passe d'accès à vos comptes.

Nous sommes heureux de vous compter parmi nos nouveaux clients.

Le service juridique  
servicejuridique@mabanques.com

Document 2 Extrait du fichier log du serveur FTP

```
(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
```

Document 3 L'interface de configuration du serveur FTP