PRESERVER L'IDENTITE NUMERIQUE DE L'ORGANISATION (1)

L'organisation cliente

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 transactions 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.

Le prestataire informatique

La DSI de M@Banque, implantée à Strasbourg, compte 20 collaborateurs. Dirigée par M. Legros, elle compte un pôle dédié à la protection de l'identité numérique de la société. Ce pôle est constitué de quatre salariés à temps plein, en relation constante avec M^me^ Schmitt, *community manager* de M@Banque. Cette dernière a notamment pour mission de gérer la communication de M@Banque sur les différents réseaux sociaux et sur le site vitrine de l'entreprise. Formée au droit de la preuve électronique et à la protection de l'identité numérique des organisations, elle veille au respect de la législation. En cas d'atteintes extérieures, elle contribue à la conception de solutions techniques avec le pôle dédié.

Cahier des charges

Deux récentes cyberattaques – la défiguration du site commercial et une tentative d'hameçonnage des courriels – ont fait apparaître les vulnérabilités du système d'information de ma M@Banque et inquiètent les clients.

À la suite de la défiguration qui a modifié l'apparence du site, la DSI a pour objectif de rétablir la e-réputation de M@Banque. Elle souhaite déployer les moyens techniques et juridiques appropriés : mise en place de solutions techniques permettant de protéger l'identité numérique de M@Banque, supports appropriés de preuves électroniques.

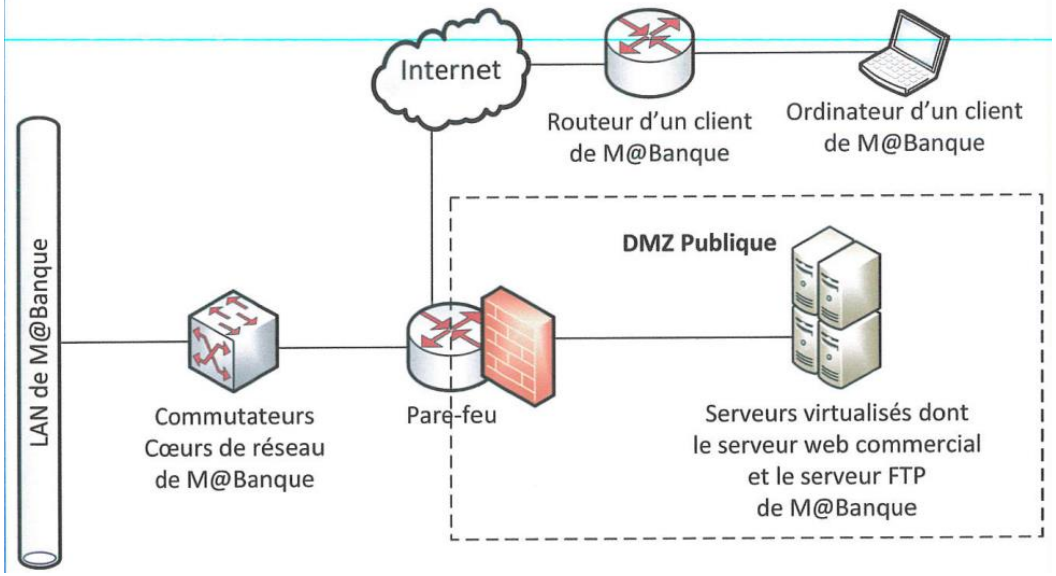
Cette mission nécessite l'association de compétences techniques et juridiques.

Situation professionnelle

Pour les clients d'une néobanque comme M@Banque, qui n'ont pour interlocuteurs que des interfaces numériques, la confiance dans la sécurité informatique est primordiale.
Deux événements majeurs ont mis à mal la sécurité du système informatique de M@Banque : la défiguration par des hackers du site commercial de la société et la réception par les clients de courriels frauduleux au nom de la société. Le *community manager* de M@Banque vous informe que de nombreux messages sur les réseaux sociaux relaient ces récents événements en dénonçant la faiblesse de la sécurité informatique de la société. Ils contribuent ainsi à en détériorer l'e-réputation. Vous êtes chargé(e) de faire le diagnostic de la situation pour chacun des événements (*hacking* et courriels frauduleux) afin de trouver des solutions technologiques pour améliorer la protection de l'identité numérique de M@Banque et rétablir la confiance de ses clients.

Description du SI de l'organisation

Schéma général du réseau de M@banque



Votre mission

Vous êtes nouvellement recruté(e) dans le pôle Protection de l'identité numérique de la DSI de M@Banque. Votre bureau est situé près de celui de M^me^ Schmitt, *community manager*. Ensemble, vous mettez en place des solutions techniques permettant de protéger l'identité numérique de M@Banque.

VIDÉO

Caractéristiques et avantages d'une néobanque

www.lienmini.fr/6988/2001

Déployer des moyens de preuves sécurisés et conformes à la législation

1. Importez les deux machines virtuelles dans votre logiciel de virtualisation (par exemple, VirtualBox) afin d'obtenir l'environnement de test.
   > Document 1
   > Machines virtuelles à importer : www.lienmini.fr/6988-301

2. Paramétrez les comptes de messagerie client ThunderBird sur les deux machines virtuelles :
   - créer les deux adresses de messagerie (M@Banque et celle du client) ;
   - créer un compte de messagerie dans ThunderBird pour chaque utilisateur ;
   - télécharger le module pour choisir le français comme langue de l'interface : Français Language Pack ;
   - ajouter le module complémentaire Enigmail dans ThunderBird afin d'intégrer le chiffrement PGP dans ThunderBird ;
   - dans le module complémentaire Enigmail, aller dans Gestion des clés et modifier les phrases de passe pour les clés de chaque utilisateur.

   > Document 2

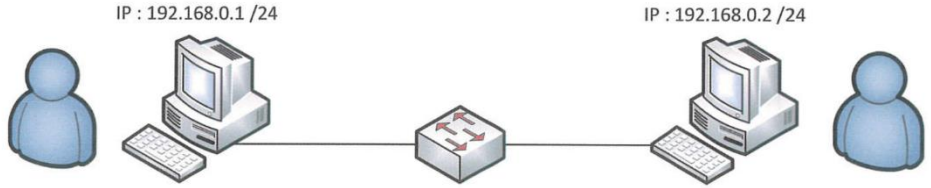
3. Testez l'envoi de courriels entre les deux acteurs et vérifiez si le contenu du message est crypté.
   > Document 3

4. Téléversez les clés publiques sur un serveur de clés dédié afin d'assurer le cryptage du contenu des messages.
   > Document 4

5. Testez l'envoi de courriels cryptés entre les deux utilisateurs en indiquant les éléments qui permettent de vérifier si l'envoi est bien sécurisé.
   > Document 4

6. Rédigez un rapport sur les tests réalisés qui démontre que l'utilisation du chiffrement PGP répond à un besoin de renforcement des moyens de preuves sécurisés.

Document 1 Le schéma réseau de l'environnement de tests



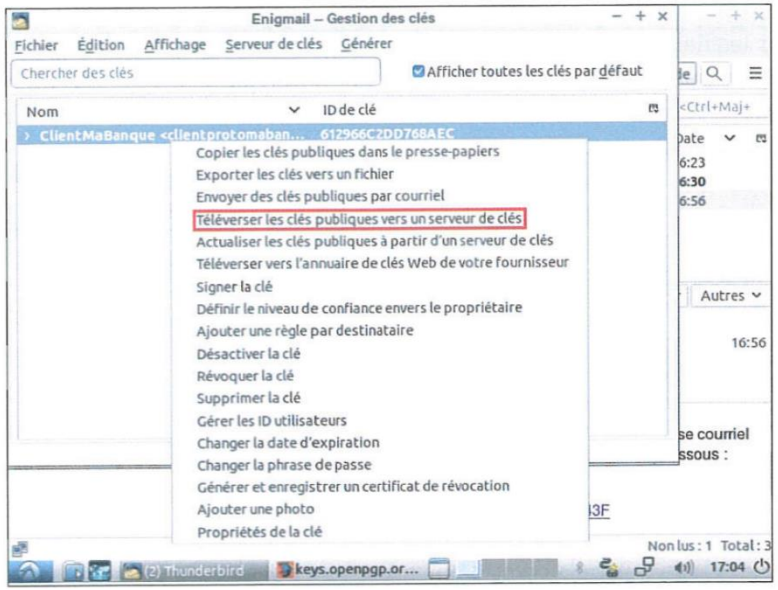
Lors de votre mission précédente, vous avez réalisé une veille sur les technologies qui permettent de crypter les contenus de courriels PGP. Votre responsable vous demande maintenant de mettre en œuvre cette technologie dans un environnement prototypé. Les conclusions de vos analyses permettront de renforcer les moyens de preuves sécurisés.

Document 2 Le cahier des charges de l'environnement de tests

Machine virtuelle « M@Banque »	Machine virtuelle « client de M@Banque »
Système d'exploitation : Debian	Système d'exploitation : Debian
Client de messagerie : ThunderBird	Client de messagerie : ThunderBird
Nom du compte de messagerie : MaBanque	Nom du compte de messagerie : ClientMaBanque
Adresse courriel à créer : (exemple : protomabanque@gmail.com)	Adresse courriel à créer : (exemple : clientprotomabanque@gmail.com)
Phrase de passe pour le chiffrement PGP : mabanque	Phrase de passe pour le chiffrement PGP : clientmabanque

Document 3 Téléverser les clés publiques vers un serveur de clés

Première étape
Téléverser une clé publique sur le serveur de clés



Seconde étape
Rechercher une clé publique sur le serveur de clés