Charpenay Côme Sio 1
27/11/25

B1 TP Compte Rendu

B3 Exercices Applications

Sommaire :

1. Composante Identité Numérique

La composante d'identité numérique visée par la cyberattaque de Tradec est une copie à l'identique du site Tradec en vue de récupérer des noms d'utilisateurs et mot de passe.

2. Étape CyberAttaque Tradec

Un serveur dirigé des requêtes vers un site Marocain hébergé en Belgique, usurpant l'identité de Tradec. Pour cela le serveur DNS a été infecté par une méthode de Poisoning, ce serveur DNS relié les correspondances d'adressage IP ainsi celle du nom de domaine du site a été remplacé par celle du site frauduleux.

1. Maquette de l'environnement

Création du réseau TRADEC avec deux commutateurs, un routeur, un serveur DNS(relié au commutateur 1), un poste salarié et un poste pirate. Ajout d'un serveur web légitime et d'un serveur web pirate relié au commutateur 2

2. Mise en place de l'environnement

Configuration ip des postes (ip, passerelle, DNS). Installation du service dns (linux ou Windows) sur le serveur tradec. La mise en place de 2 vlans différents avec activation d'un routage inter vlans. Le routeur doit permettre le trafic entre réseau Tradec et internet.

3. Script d'empoisonnement DNS

172.16.1.1 -> site officiel
172.16.1.2 -> site pirate

Le pirate va changer l'adresse qui redirige vers le site web de tradec en tapant la commande netsh interface ipv4 set adresse nom = "Site Tradec" statique 172.16.1.2 255.255.0.0 172.16.1.254 **dans le cmd en mode administrateur.**

4. Tests d'accès

Depuis le poste du salarié nous réaliserons des tests avant attaque -> accès au vrai site. Puis des tests après attaque pour permettre la redirection vers le site frauduleux et ainsi pouvoir vérifier la mise en place de l'empoisonnement du serveur dns.

5. Synthèse et sécurisation

L'empoisonnement DNS permet de détourner les utilisateurs vers un faux site.Les solutions à adopter sont de sécuriser le serveur DNS, de restreindre les accès, utilisés DNSSEC, de surveiller les modifications et isoler les postes suspects. Il serait intéressant d'intégrer des pare-feu (liste blanche, liste noir) sur le réseau ainsi que des restrictions aux niveaux des requêtes en fonction des postes salariés. Cela permettrait une sécurité plus poussée.

1. Les Conditions de la Signature Électronique

Les signatures électroniques sont aussi recevable qu'un écrit papier en respectant certaines conditions. Tel que le faites d'être gérées par les banques grâce à des logiciels de signature (sur téléphone ou ordinateur) en identifiant l'identité par l'établissement bancaire ainsi qu'une clé privée et clé publique (cryptant et décryptant la signature). Cependant il faut également que la signature dématérialisé soit conforme aux articles 1316-1 et 1666 du Code Civil en France, c'est à dire que l'auteur soit clairement identifié; que le lien entre l'acte et la personne soit garantit; que l'intégrité de l'écrit signé est assuré; que le client est bien manifesté son consentement aux obligations de l'acte.

2. Le Rôle de la Signature Électronique

Le rôle associé à la signature électronique est de créer une empreinte numérique grâce au logiciel, pour composée d'une suite de lettres et de chiffres codé grâce à la clé privée contenue dans un certificat numérique. Ce certificat numérique permet d'assurer l'identité du contractant dans son engagement dans un contrat ou une action certifiant son accord. De plus il est possible de vérifier l'identité du contractant sur le logiciel grâce au à la clé public (clé fournie lors du contrat) et la clé privé (clé dans la base de donnée du logiciel)donnant l'identité du client.

3. Analyse des Avantages Signature Électronique

Les avantages que propose la signature électronique est de permettre une accessibilité aux contrats et actions plus efficace et efficiente par le fait de pouvoir s'engager n'importe où (en ligne) avec facilité (ex: moins de démarches/papiers), ainsi que de passer par une automatisation des procédures faisant gagner énormément de temps.

4. Identification des Risques Signature Électronique

Les risques pouvant être rencontré par Fortuneo lors de l'utilisation de la signature électronique pour l'acte de souscription sont :

Usurpation d'identité

Sans authentification forte, une personne malveillante pourrait souscrire un ou plusieurs contrats à la place d'un client.

Contestations juridiques du contrat par le client

Le client pourrait nier avoir signé le contrat : sans signature électronique « qualifiée », la preuve de son consentement serait difficile à revendiquer .

Fraude du Contrat

Des documents signés pourraient être falsifiés ou modifiés sans que la banque ne s'en aperçoive. Également des modifications de clé privée dans la base de donnée

Non-respect des obligations légales

La banque doit garantir l'intégrité et l'authenticité des actes (Article 1316-1 et 1366): sans signature électronique conforme aux normes du Code civil, elle pourrait être en infraction et alors Fortuneo pourrait rencontrer des problèmes judiciaires..

Atteinte à l'intégrité des données clients

Les informations contenues dans le contrat pourraient être altérées sans système de cryptage sécurisé (ex: AES).

Rejets ou annulations de contrats

Les contrats pourraient être invalidés, car dépourvus d'une procédure de signature reconnue juridiquement.

Perte de confiance des clients et mauvaise image de Fortuneo

Un processus peu sécurisé pourrait dissuader les clients, nuisant à la réputation et au développement de la banque en ligne.