Lucas Da Silveira B1

Projet Sécurité

Tâche 1 :

Sujet : En 2013, Yahoo a été victime d'une importante violation de données qui a touché environ 3 milliards de comptes d'utilisateurs. L'incident a été l'une des plus grandes failles de sécurité dans l'histoire d'Internet.

1.
L'attaque contre Yahoo a été attribuée à des acteurs soutenus par un État, selon les investigations. Les attaquants ont profité d'une insuffisance en matière de sécurité malgré un hachage bcrypt pour protéger les mots de passe, de plus ils exploitaient une vulnérabilité dans la création et la gestion des cookies d'identification des utilisateurs en utilisant des « forged cookies » qui permettaient aux attaquants d'accéder aux comptes des utilisateurs sans nécessiter de mot de passe.

2.
L'impact de cette violation de données était considérable. Les informations compromises incluaient des noms, des adresses e-mail, des numéros de téléphone, des dates de naissance et des mots de passe cryptés. Les conséquences pour les individus allaient de la perte de confidentialité à des risques accrus de vol d'identité. Pour Yahoo, cela a entraîné une perte de confiance de la part des utilisateurs, des enquêtes réglementaires et des répercussions financières significatives.

3.
Yahoo a pris des mesures pour résoudre l'incident en prenant conscience de la faille de sécurité. L'entreprise a mis en œuvre des améliorations dans ses pratiques de sécurité, a informé les utilisateurs affectés et les a encouragés à changer leurs mots de passe. Yahoo a également coopéré avec les autorités compétentes et a renforcé ses mesures de sécurité pour éviter de futures violations.

Tâche 2 :

1.
Informations personnelles : nom, adresse, numéro de téléphone, date de naissance.
Informations financières : numéros de carte de crédit, informations bancaires.

2.
Serveurs de base de données.
Serveurs d'application.
Réseau interne.
Interfaces utilisateur et applications.

3.
Risques : vol d'identité, fraude financière.
Menaces : attaques par force brute, phishing, accès non autorisé.
Vulnérabilités : failles de sécurité logicielle, insuffisances dans le contrôle d'accès

4.
Authentification forte : utilisation de l'authentification à deux facteurs.
Contrôle d'accès strict : accès basé sur les rôles et les privilèges.
Système de détection d'intrusion (IDS) : surveillance continue du trafic réseau.
Chiffrement des données : stockage et transmission sécurisés des informations sensibles.
Mises à jour régulières des logiciels : correction des vulnérabilités connues.

5.
Stratégies de communication : informer rapidement les parties prenantes et les utilisateurs affectés.
Procédures d’escalade : définir des canaux de communication et des responsabilités pour une réponse rapide.
Étapes d’analyse post-incident : enquête approfondie pour comprendre la nature de l'incident.
Améliorations post-incident : ajuster les politiques de sécurité, renforcer les mesures de prévention.