TRAVAUX PRATIQUES

TP– SCENARII ATTAQUE PAR RANSOMWARE

I. INTRODUCTION

1.1 A propos de ce TP.

Objectif :

1. **Compréhension des attaques par ransomware** : Apprendre comment les attaques par ransomware sont menées et quelles sont leurs conséquences sur une entreprise.
2. **Évaluation de l'impact** : Savoir évaluer l'ampleur d'une attaque et identifier les systèmes compromis.
3. **Réponse à l'incident** : Développer des compétences pour coordonner une réponse technique efficace et minimiser les impacts de l'attaque.
4. **Collaboration inter-départements** : Travailler en équipe avec différents rôles (RSSI, DSI, PDG, etc.) pour gérer la crise.
5. **Communication de crise** : Apprendre à gérer la communication avec les parties prenantes internes et externes, y compris les médias.
6. **Prise de décision stratégique** : Savoir prendre des décisions critiques sous pression, comme payer ou non la rançon.
7. **Mise en œuvre des mesures de sécurité** : Appliquer des mesures de confinement et de restauration des systèmes à partir des sauvegardes.
8. **Interaction avec les autorités et les experts** : Collaborer avec les autorités et les experts en cybersécurité pour résoudre l'incident.

2. CONTEXTE

La société "Global Donuts" est une entreprise internationale de vente de donuts, avec son siège social en France. Toutes les machines de la société, y compris celles des boutiques, sont ciblées par une attaque par ransomware. Seul un poste dans l'entreprise centrale n'est pas chiffré, et un fichier nommé "Readme.txt" est trouvé sur le poste du PDG.

2.1 Jeux de rôles

Vous devez vous mettre dans la peau de chaque personnage suivant :

Rôles des étudiants

1. **RSSI (Responsable de la Sécurité des Systèmes d'Information)**
    - **Description du rôle** : Responsable de la sécurité des systèmes d'information de l'entreprise. Doit évaluer l'ampleur de l'attaque, coordonner la réponse technique et travailler avec les autres départements pour minimiser les impacts.
    - **Actions possibles** :
        - Analyser l'attaque et identifier les systèmes compromis.
        - Mettre en place des mesures de confinement.
        - Collaborer avec les autorités et les experts en cybersécurité.
2. **DSI (Directeur des Systèmes d'Information)**
    - **Description du rôle** : Responsable de la gestion des systèmes d'information de l'entreprise. Doit superviser la réponse à l'attaque et assurer la continuité des opérations.
    - **Actions possibles** :
        - Coordonner avec le RSSI pour évaluer l'impact sur les opérations.
        - Communiquer avec les fournisseurs de services IT pour obtenir de l'aide.
        - Élaborer un plan de reprise d'activité.
3. **PDG (Président Directeur Général)**
    - **Description du rôle** : Responsable de la direction générale de l'entreprise. Doit prendre des décisions stratégiques et communiquer avec les parties prenantes.
    - **Actions possibles** :
        - Décider de payer ou non la rançon.
        - Communiquer avec les actionnaires et les employés.
        - Travailler avec l'équipe de communication pour gérer la crise.
4. **Gestion de la communication de presse**
    - **Description du rôle** : Responsable de la communication externe de l'entreprise. Doit gérer les relations avec les médias et informer le public de la situation.
    - **Actions possibles** :
        - Préparer des communiqués de presse.
        - Répondre aux questions des médias.
        - Gérer la communication sur les réseaux sociaux.

5. **Technicien**
    - **Description du rôle** : Responsable de l'assistance technique. Doit aider à la mise en œuvre des mesures de réponse et de reprise.
    - **Actions possibles** :
        - Appliquer les mesures de confinement.
        - Restaurer les systèmes à partir des sauvegardes.
        - Assister le RSSI et le DSI dans leurs tâches.

2.2 Comment auriez-vous pu éviter l'attaque selon vous !

Décrire le schéma logique de la mise en œuvre des bonnes pratiques SSI.

Comment feriez-vous pour sécuriser l'infrastructure.