ANALYSE DE RISQUES

1: Identification de risques :

3.1 : Les 5 sources de risque de l'association et les objectifs visés sont :

Les données de carte bancaire sont des données sensibles et intéressent donc les hackers pour faire des transactions avec ses informations.

- Internet peut apporter des malwares, et un client peut être victime d'une tentative de phishing sur internet pour avoir accès au poste.
- Un VLAN mal configuré peut donner un accès privilégié à des personnes malveillantes pour qu'elles puissent avoir accès à des informations personnelles/sensibles/confidentielles pour les vendre ou les exploiter.
- La fibre optique ne peut pas être sécurisée physiquement de partout, un hackeur pourrait y accéder pour couper le câble et donc interrompre les communications pour ralentir une attaque phishing par exemple.
- Le wifi peut être piraté s'il n'est pas correctement chiffré ou que la sécurité n'est pas renforcée (comme le mot de passe), toutes les données partagées seront visibles par l'hackeur.

3.2 : Les biens essentiels nécessitant une protection sont :

- Le routeur pour une connexion internet sécurisé.
- VLAN
- La fibre optique
- Les quarts points d'accès wifi
- Les six serveurs pour sécuriser les données de carte bancaire.

3.3 : Classification de risques :

1) Les données de cartes bancaires car ce sont des données sensibles donc les plus recherchées sur internet.
2) Internet car des malwares et des tentatives de phishing sont nombreuses.
3) VLAN car des données sensibles peuvent être accessible par des personnes non autorisées.
4) Fibre optique car le réseau peut être compromis.
5) Wifi car le trafic peut être intercepté.

2: Scénario d'attaque :

1. Un mail frauduleux est envoyé sur la boite mail d'un salarié pour lui informer que son colis arrive bientôt. Il clique sur le lien pour suivre son avancé et un malware s'installe sur son poste pour le contrôler à distance et compromettre les données sensibles si le salarié a accès et la continuité des opérations. La vraisemblance est très élevée car le phishing est très fréquent.

2. Un hackeur va envoyer un grand nombre de requêtes au serveur DNS pour saturer sa bande passante et donc rendre impossible la communication entre Internet et le réseau. La vraisemblance est moyenne, les attaques DDoS sont fréquentes mais pas toujours réussies.
3. Un hackeur intercepte le mot de passe chiffré (diffusé tout le temps par les routeurs) et utilise la force brute pour le déchiffrer et avoir accès à tous les échanges fait sur le réseau pour supprimer des données par exemple. La vraisemblance est moyenne car ça dépend de la solidité des mots de passe.

3: Traitement des risques :

3.4 : Stratégie de traitement et mesures conseillées :

- On évite la fuite des données de carte bancaire car c'est un trop gros risque financier et réputationnel pour l'entreprise. Pour éviter cela, une tokenisation et le chiffrement des données pourrait être mise en place.
- On évite le risque de malwares et de phishing sur internet car il est très fréquent. Pour éviter cela, des antimalware et antivirus pourraient être mis en place avec une formation des employés sur les mails frauduleux.
- On réduit le risque d'accessibilité des personnes (VLAN). Pour éviter cela, une segmentation du réseau pourrait être mis en place.
- On accepte le risque de la fibre optique car il faut être présent physiquement, ce qui est rare. Pour éviter cela, des verrous sur les équipements sensibles pourraient être mis en place.
- On réduit le risque du Wifi car mettre des mots de passe robuste suffit.

3.5 : Plan de mise en œuvre pour les mesures de sécurité :

1. Protection des données bancaires :
    - Utiliser AES-256 (protocole de chiffrement pour un transfère sécuriser) pour les données de transaction de carte bancaire.
    - Remplacer les données sensibles par des tokens dans la base de données.
    - Equipe de sécurité informatique.
    - Audits tous les 3 mois.
2. Malwares et Phishing :
    - Installer et configurer des antimalwares et des antivirus sur tous les postes.
    - Organiser une formation pour tous les employés sur les techniques de phishing employées.
    - Equipe de sécurité.
    - Formations pour les nouveaux employés.
3. VLAN :
    - Configurer les VLAN pou isoler les parties du réseau.

- Administrateur réseau.
- Surveillance continue.

4. Fibre optique :
    - Mettre des verrous sur les équipements sensibles.
    - Gestionnaire des installations
    - Suivi continu.
5. Wifi :
    - Créer des mots de passes de plus de 12 caractères avec des majuscules, des minuscules, des nombres et des caractères spéciaux.
    - Administrateur réseau.
    - Renouvellement des mots de passe tout les 6 mois.