Document sur les Scénarios Malveillants et les Contre-mesures (Evil users stories)

Scénario Malveillant 1 : Vol de Données Clients

Description du Scénario :

Un attaquant parvient à accéder aux bases de données de Sushill.fr et vole les données clients, y compris les adresses e-mail, les historiques de commande et d'autres informations personnelles. Ces données peuvent être utilisées à des fins de spam, de phishing ou de fraude.

Contre-mesures :

1. **Cryptage des Données** : Toutes les données clients stockées sur les serveurs de Sushill.fr doivent être cryptées pour empêcher tout accès non autorisé. Le cryptage fort des données sensibles rendra leur accès beaucoup plus difficile pour les attaquants.
2. **Sécurisation des Accès** : Mise en place de mesures de sécurité renforcées pour limiter l'accès aux bases de données. Cela peut inclure l'utilisation de mots de passe forts, l'authentification à deux facteurs, et la limitation des privilèges d'accès aux seules personnes autorisées.
3. **Surveillance des Activités Anormales** : Mise en place d'un système de surveillance des activités suspectes sur le site web. Cela permettra de détecter rapidement toute tentative d'accès non autorisé ou de comportement anormal dans la manipulation des données.
4. **Mise à Jour Régulière des Systèmes** : Assurer que tous les logiciels et systèmes utilisés sur Sushill.fr sont régulièrement mis à jour avec les derniers correctifs de sécurité pour réduire les vulnérabilités potentielles aux attaques.

Scénario Malveillant 1 :Accès Non Autorisé à l'API REST

Description du Scénario :

Un client malveillant parvient à accéder à l'API REST de Sushill.fr, compromettant l'intégrité des données et la sécurité du système en modifiant, supprimant ou ajoutant des données client.

Contre-mesures :

1. **Authentification et Autorisation Fortes** : Utilisation de mécanismes robustes d'authentification et d'autorisation pour vérifier l'identité des utilisateurs et limiter leur accès aux seules opérations autorisées.

2. **Validation des Données et des Requêtes** : Mise en place de contrôles pour valider les données entrantes et les requêtes API afin de détecter et rejeter les activités suspectes.
3. **Cryptage des Données Sensibles** : Chiffrement des données sensibles transmises via l'API pour garantir leur confidentialité.
4. **Surveillance et Analyse des Activités** : Surveillance du trafic API pour détecter les comportements anormaux et analyse des journaux d'activité pour identifier les tentatives d'accès non autorisé.
5. **Mise à Jour Régulière** : Assurer la mise à jour régulière des composants logiciels pour corriger les vulnérabilités et minimiser les risques d'exploitation.