Cybersécurité Drone Mission A Elisée

Mission A

Mission 1

* 1. Scénario 2 : Un problème technique peut survenir lors du transfert de données du drone vers le SSD, les données peuvent ainsi être corrompues, cela risque d’entraîner un risque pour l’intégrité.

Scénario 3 : Une personne non autorisée à accéder aux données arrive à se connecter au serveur FTP où les données sont collectées. La personne peut alors modifier les données ou les copier. Cela représente un risque pour la disponibilité et pour la confidentialité.

1.2

Niveaux de vraisemblance d’une menace

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Source de menace | Type de menace | Bien support | Niveau de vraisemblance | Critère de sécurité mis en jeu | | | | |
| C | D | | I | |
| Scénario 2 | Menace non intentionnelle | Carte SSD | 3- Important Les problèmes techniques lors des transferts des données sont courant |  |  | | X  Les données peuvent être corrompues | |
| Scénario 3 | Menace intentionnelle | Serveur FTP | 3- Important Si le serveur FTP est mal sécurisé, il peut être la cible d’attaque | X  La confidentialité n’est pas respectée si une personne non autorisé a accès aux données | | X  L’attaquant peut s’attaquer aux données et les rendre indisponible | |  |

Niveau de gravité d’un risque

|  |  |  |
| --- | --- | --- |
| Scénario 2 | Problème technique | Niveau de gravité : 3  La corruption des données peut entraîner une perte de confiance des clients ainsi que des risques financiers pour l’entreprise |
| Scénario 3 | Attaque serveur FTP | Niveau de gravité : 3  Un accès non autorisé peut entrainer la divulgation ainsi que l’altération des données sensibles ce qui peut présenter la perte de confiance des clients ainsi que des problèmes juridiques et financier. |

1.3

Scénario 1 : La mise en place d’un disque SSD supplémentaire permettant d’avoir une sauvegarde supplémentaire si le 1er disque rencontre un problème.

Scénario 2 : Drone sécurité devrait mettre en place des contrôles pour l’intégrité des données lors du transfert vers la carte SSD, tel que la vérification du transfert et de l’état du disque, ainsi que l’ajout d’un disque dur supplémentaire.

Scénario 3 : Il faudrait renforcer la sécurité du serveur FTP avec la mise en place du chiffrement et en limitant l’accès aux personnes autorisées.

2.1

Le 1er engagement qui garantit la non-réutilisation des données hébergées sur les services. Cela renforce la protection des données en empêchant l’utilisation à des fins non autorisées.

2.2

L’acteur responsable de la publication d'images privées sur le site de l'exploitant est l'exploitant agricole lui-même.

2.3

Il faut mettre en place un système de contrôle et d’autorisation. Il faut également mettre en place l’utilisation de mot de passe sécurisés et fort ainsi que la vérification d’identité. Il peut également y avoir une sensibilisation aux bonnes pratiques de protection des données. Renforcer les mesures de sécurité du serveur FTP, et la mise en place d’un processus de gestion des incidents en cas de violation des données, en notifiant les personnes concernées et les autorités.