Voltron Greentech

Sécurité du système d’information et des l’applications

Ce document tente de répondre au besoin de sécurité des systèmes et des applications liées aux Vignerons Indépendants en proposant des solutions et recommandations pour les différents services et systèmes.

OBJECTIFS

1. Toutes les données sont considérées comme sensibles et doivent être sécurisées et cryptées, de leur collecte à leur traitement, sans exception.
2. La solution doit également être accompagnée d'instructions de sécurité claires.
3. La gestion des droits doit optimiser la sécurité et éviter les erreurs involontaires.

Besoin 1 : Sécurisation des données

1. **Collecte des données :**
    - Utilisation de protocoles sécurisés (HTTPS) pour collecter les données afin de garantir une communication cryptée entre les utilisateurs et votre système.
    - Garantir la présence de certificats valides et de confiance lors des échanges.
    - Évitez au maximum la collecte de données sensibles à moins qu'elles ne soient strictement nécessaires, et en informer les utilisateurs au cas échéant.
2. **Stockage des données :**
    - Utilisation d’une base de données sécurisée pour stocker les données collectées.

- Utilisation de MySQL Enterprise Transparent Data Encryption (TDE) afin de crypter directement la base de données en temps réel et au niveau du disque dur.

3. **Traitement des données :**
   - Utilisation de protocoles sécurisés lors des échanges de données.
   - Si utilisation de services tiers : s'assurer qu'ils respectent la même politique de sécurité des données.
   - Appliquez des contrôles d'accès stricts pour s'assurer que seules les personnes autorisées peuvent accéder aux données sensibles.

4. **Cryptage des données :**
   - Utilisation d'algorithmes de cryptage robustes pour crypter les données sensibles telles que les mots de passe. L'algorithme AES (Advanced Encryption Standard) est largement recommandé.
   - Stockage des clés de cryptage de manière sécurisée, en utilisant des méthodes de gestion des clés appropriées, telles que des systèmes de gestion de clés (KMS).

Besoin 2 : Instruction de sécurité lié à la solution et aux systèmes

1. **Documentation technique :**
   - Élaboration d'une documentation technique détaillée décrivant les protocoles et technologies utilisés.
   - Expliquez clairement les implications des échanges de données.
2. **Développement de solutions sécurisées :**
   - Utilisation d'outils permettant la reconnaissance de vulnérabilités sur la base de code tel que Snyk.
   - Revue de code par plusieurs personnes lors de la sortie d'une nouvelle fonctionnalité.
   - Assurez-vous que les formulaires de collecte de données sont sécurisés et protégés contre les attaques courantes telles que les injections SQL ou les attaques par script intersite (XSS).
   - Confirmation à la politique de sécurité globale (journaux de logs ...)

3. **Formation et sensibilisation :**
    - Organisation de sessions de formation pour les utilisateurs et le personnel technique sur les bonnes pratiques de sécurité.
    - Sensibilisez les utilisateurs aux risques associés à la mauvaise gestion des droits, tels que les fuites de données ou les accès non autorisés.
4. **Procédures d'urgence :**
    - Développement d’un plan de procédures d'urgence (PRA) pour faire face à d'éventuelles violations de sécurité.
    - Précisez les actions à prendre en cas de compromission des droits d'accès ou de détection d'une activité suspecte.
5. **Contrôles et audits réguliers :**
    - Recommandation de la réalisation régulière de contrôles et d'audits de sécurité pour vérifier la conformité aux politiques et procédures de sécurité.
    - Explication des étapes à suivre pour effectuer ces contrôles et audits, et encourager une culture responsable.
6. **Centre d’opérations de sécurité (SOC)**
    - Mise en place d’un centre d’opérations et de sécurité, en interne ou en externe suivant les besoins.
    - Mise en place d’un outil de gestion des logs tel que la suite ELK.
    - Fournissez des canaux de communication clairs pour que le SOC puisse intervenir rapidement en cas d’incident.

Besoin 3 : Gestion des droits

1. **Modèle de contrôle d'accès :**
    - Mise en place d’un modèle de contrôle d'accès basé sur le principe du moindre privilège (Principle of Least Privilege, PoLP). Cela signifie que chaque utilisateur ou système ne doit avoir que les droits d'accès nécessaires pour effectuer ses tâches spécifiques.
    - Utilisation de groupes de sécurité pour regrouper les utilisateurs ayant des besoins d'accès similaires. Cela facilitera la gestion des droits en attribuant des autorisations aux groupes plutôt qu'aux utilisateurs individuels.

2. **Contrôles de validation et de séparation des tâches :**
    - Mettez en place des contrôles de validation pour les opérations sensibles. Par exemple, exigez une approbation ou une vérification supplémentaire (un code par mail par exemple) avant d'accorder des droits d'accès sensibles ou d'effectuer des actions critiques.
    - Séparez les tâches critiques en utilisant le principe de séparation des tâches (Separation of Duties, SoD). Cela signifie que des actions sensibles nécessitent l'intervention de plusieurs utilisateurs ou équipes distinctes pour minimiser les risques d'abus ou d'erreurs.
3. **Revue régulière des droits d'accès :**
    - Il faut régulièrement faire des revues de droits d'accès pour assurer que ceux-ci soient toujours pertinents et appropriés. Révoquer les droits d'accès inutilisés ou obsolètes pour réduire la surface d'attaque potentielle.
4. **Journalisation et suivi des activités :**
    - Mettre en place un système de journalisation pour enregistrer les activités liées aux droits d'accès, telles que les modifications de permissions ou les tentatives d'accès non autorisées.
    - Surveiller régulièrement les journaux d'activité pour détecter les anomalies ou les comportements suspects et prendre les mesures nécessaires en cas d'incident de sécurité.