**Etude des Besoins - Authentification**

1. **Identification des Parties Prenantes**

* Responsables des processus Métier : Délégué à la Protection des Données – KONTE Amara
* Responsables Informatique : Directeur Cybersécurité – GOMIS Kwency
* Utilisateur : Tous les employés.

1. **Collecte des Exigences**

***Disponibilité - Le système d'information doit être disponible 99,9% du temps***

*Quels sont les services, systèmes ou données critiques pour l’organisation ?*

* *Serveur : odysath01p*
* *Réseaux : 001-int-prd-odys*
* *Données : Informations Clients, Bases de Données.*

*Quels sont les conséquences d’une perte de disponibilité ?*

*Aucune accessibilité aux ressources de l’entreprise*

***Intégrité - Assurer l'intégrité des données sensibles***

*Quels sont les processus et les données qui doivent être protégés contre toute altération non autorisée ?*

*Le processus de stockage des mots de passe dans la base de données et les données : Les mots de passes*

*Comment garantir l'intégrité des données pendant leur stockage, leur transmission et leur traitement ?*

*L'ajout de couches de sécurité supplémentaires, comme l'utilisation de certificats SSL/TLS.*

***Confidentialité - Garantir la confidentialité des informations clients***

*Quelles informations sont considérées comme sensibles ou confidentielles ?*

*L’ID, Nom, Prénom, Adresse, Email, Mot de passe et Numéro de téléphone.*

*Comment assurer la confidentialité des données contre l'accès non autorisé ?*

*Ajouter une vérification d’authentification à 2 facteurs (2FA).*

***Preuve - Mettre en place des mécanismes de preuve pour les transactions critiques***

*Quelles sont les exigences en matière de préservation des preuves numériques ?*

*Avoir l’historiques des connexions et des actions de l’utilisateur (ex : modification du mot de passe)*

*Comment garantir l'intégrité et l'authenticité des preuves numériques en cas d’incident ?*

*Grâce à l’historique protégé et conservé pendant 5 ans.*

*Choix de notre DICP et Criticité au vu de notre besoin :*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Disponibilité** | **Intégrité** | **Confidentialité** | **Preuve** | **Criticité** |
| 04 - Majeur | 04 - Majeur | 04 - Majeur | 04 - Majeur | 03 - Stratégique |

1. **Évaluation des Ressources**

Voici les ressources disponibles :

* *Equipe Cybersécurité*
* Serveurs : odysath01p
* Réseaux : 001-int-prd-odys
* *Financières : 350€/an + maintenance*

1. **Conformité Réglementaire**

**Principe de Licéité, Loyauté, et Transparence (Article 51 - a) :**

* Informer les utilisateurs de manière transparente sur la collecte et le traitement de leurs données d'identification.
* Obtenir le consentement explicite des utilisateurs pour le traitement de leurs données d'authentification.

**Limitation des Finalités (Article 51 - b) :**

* Collecter et traiter uniquement les données d'authentification nécessaires à des fins spécifiques et légitimes.
* Éviter la collecte excessive de données.

**Minimisation des Données (Article 51 - c) :**

* Collecter uniquement les données d'authentification nécessaires à la finalité spécifique.
* Éviter de stocker des informations excessives.

**Exactitude des Données (Article 51 - d) :**

* Mettre en place des procédures pour assurer l'exactitude des données d'authentification.
* Permettre aux utilisateurs de mettre à jour leurs informations d'identification.

**Limitation de la Conservation (Article 51 - e) :**

* Établir des délais de conservation clairs pour les données d'authentification.
* Supprimer les données d'identification lorsque leur conservation n'est plus nécessaire.

**Intégrité et Confidentialité (Article 51 - f) :**

* Mettre en place des mesures de sécurité appropriées pour assurer l'intégrité et la confidentialité des données d'authentification.
* Utiliser des méthodes de stockage sécurisées et chiffrer les données sensibles.

**Responsabilité Active (Article 24) :**

* Désigner un délégué à la protection des données (DPO) si cela est nécessaire en fonction de la taille et de la nature du traitement des données.
* Réaliser des évaluations d'impact sur la protection des données (EIPD) si le traitement présente un risque élevé.

**Sécurité du Traitement (Article 32) :**

* Mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque.
* Effectuer des tests de sécurité réguliers et assurer de la résilience du système d'authentification.

**Notification des Violations de Données (Article 33) :**

* Élaborer un processus de notification des violations de données et informer rapidement l'autorité de contrôle compétente en cas de violation.

**Droits des Personnes Concernées (Articles 15-22) :**

* Respecter les droits des individus en ce qui concerne l'accès, la rectification, la suppression et la portabilité de leurs données d'authentification.

**Privacy by Design et by Default (Article 25) :**

* Intégrer des principes de protection des données dès la conception et par défaut dans le développement du système d'authentification.

1. **Elaboration d’un Cahier des Charges**

**Installation d’application 2FA sur une machine virtuelle**

1. **Installer Google Authenticator (ou une autre application 2FA) :**
   * Installer une application d'authentification à deux facteurs comme Google Authenticator, Authy, ou Microsoft Authenticator sur la machine virtuelle.
2. **Activer la 2FA sur le compte utilisateur :**
   * Assurer que la 2FA est activée pour le compte utilisateur sur la machine virtuelle. Cette configuration peut être différente en fonction du système d'exploitation.
3. **Configurer le compte 2FA :**
   * Accéder aux paramètres de sécurité du compte utilisateur.
   * Trouver l'option "2FA" ou "Authentification à deux facteurs" et l'activer.
   * Suivre les instructions pour associer l'application 2FA au compte. Cela impliquera généralement de scanner un code QR avec l'application 2FA.
4. **Sauvegarder les codes de récupération :**
   * S'assurer de sauvegarder soigneusement les codes nécessaires à la récupération, tels que les codes de récupération.
5. **Tester l'authentification 2FA :**
   * Se déconnecter ou redémarrer la machine virtuelle.
   * Lors de la reconnexion, fournir le code généré par l'application 2FA.