**Etude des Besoins - Partage**

1. **Identification des Parties Prenantes**

* Responsables des processus Métier : Administrateur Système et Réseau – 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 : dysnfs01p ; odysftp02p*
* *Réseaux : 001-int-prd-odys ; 008-ext-dmz-odys*
* *Données : Fichiers Interne & Externe*

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

*Aucune accessibilité aux ressources mis à disposions*

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

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

*Les processus liés à la gestion des utilisateurs, y compris l'authentification et l'autorisation.*

*Le processus de mis à jour du logiciel ftp pour corriger les vulnérabilités.*

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

*En Utilisant les protocoles de transfert sécurisés tels FTPS (FTP sécurisé) ou SFTP (SSH File Transfer Protocol) pour chiffrer les données pendant leur transmission.*

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

*Quelles informations sont considérées comme sensibles ou confidentielles ?*

*Utilisateur et Mot de passe.*

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

*Ajouter une vérification avec les clés privées en plus des mots de passe.*

***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 : ajout d’un fichier)*

*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** |
| 02 - Significatif | 04 - Majeur | 02 - Significatif | 03 - Fort | 02 - Critique |

1. **Évaluation des Ressources**

Voici les ressources disponibles :

* *Equipe Cybersécurité*
* *Serveurs : dysnfs01p ; odysftp02p*
* *Réseaux : 001-int-prd-odys ; 008-ext-dmz-odys*
* *Financières :* **Petite entreprise :**
  + - Installation initiale (matériel, logiciels, configuration) : Entre 5 000 et 15 000 euros.
    - Coûts annuels de maintenance et de support : Entre 2 000 et 5 000 euros.
* **Entreprise de taille moyenne :**
  + - Installation initiale (matériel, logiciels, configuration) : Entre 15 000 et 50 000 euros.
    - Coûts annuels de maintenance et de support : Entre 5 000 et 15 000 euros.
* **Grande entreprise :**
  + - Installation initiale (matériel, logiciels, configuration) : Plus de 50 000 euros.
    - Coûts annuels de maintenance et de support : Plus de 15 000 euros.

1. **Conformité Réglementaire**

Lors de l'élaboration d'un serveur de partage de fichiers, que ce soit via FTP (File Transfer Protocol) ou NFS (Network File System), vous devez tenir compte des règles du Règlement général sur la protection des données (RGPD) de l'Union européenne. Voici quelques règles spécifiques à prendre en considération :

1. Consentement : Si le serveur de partage de fichiers collecte des données personnelles, assurez-vous d'obtenir le consentement des utilisateurs avant de traiter ces données. Le consentement doit être libre, spécifique, éclairé et univoque.
2. Finalité du traitement : Les données personnelles collectées via le serveur de partage de fichiers doivent être utilisées uniquement pour les finalités spécifiques pour lesquelles elles ont été collectées. Informez clairement les utilisateurs de ces finalités.
3. Minimisation des données : Limitez la collecte et le traitement des données personnelles au strict nécessaire pour atteindre les finalités définies. Évitez la collecte excessive d'informations inutiles.
4. Sécurité : Assurez-vous que le serveur de partage de fichiers et les données qu'il traite sont sécurisés. Utilisez des protocoles sécurisés comme SFTP (FTP sécurisé) et implémentez des mesures de sécurité appropriées pour protéger les données.
5. Droits des personnes concernées : Respectez les droits des individus, tels que le droit d'accès, le droit de rectification, le droit à l'effacement, le droit à la limitation du traitement, et le droit à la portabilité des données. Les utilisateurs doivent avoir la possibilité de gérer leurs propres données personnelles.
6. Notification des violations de données : En cas de violation de données personnelles présentant un risque élevé pour les droits et libertés des personnes, notifiez cette violation aux autorités de contrôle et, dans certains cas, aux personnes concernées.
7. Chiffrement des données : Utilisez des méthodes de chiffrement pour protéger les données stockées et transitant sur le serveur de partage de fichiers, réduisant ainsi le risque d'accès non autorisé.
8. Traçabilité : Maintenez des registres détaillés des activités de partage de fichiers, enregistrant notamment les accès, les modifications et les transferts de données, pour pouvoir démontrer la conformité en cas de besoin.
9. Durée de conservation : Définissez des périodes de conservation appropriées pour les données personnelles stockées sur le serveur de partage de fichiers et supprimez-les lorsque ces périodes expirent ou lorsque les données ne sont plus nécessaires.
10. Audit régulier : Effectuez des audits réguliers de la sécurité et des pratiques de traitement des données pour assurer la conformité continue aux exigences du RGPD.

Il est essentiel de s'assurer que l'infrastructure, les protocoles et les processus associés à votre serveur de partage de fichiers sont conformes aux normes de protection des données. Si nécessaire, consultez un professionnel de la protection des données ou un avocat spécialisé pour des conseils spécifiques à votre situation.

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

**Nextcloud :**

1. Préparation de la machine virtuelle :

- Créez une machine virtuelle avec les spécifications requises (RAM, espace disque, etc.).

- Installez un système d'exploitation compatible (Ubuntu, CentOS, etc.).

2. Installation de Nextcloud :

- Configurez le serveur web (Apache ou Nginx) et installez PHP avec les extensions nécessaires.

- Téléchargez et installez Nextcloud depuis le site officiel.

- Configurez la base de données (MySQL, MariaDB, PostgreSQL) pour Nextcloud.

- Suivez les instructions d'installation de Nextcloud et configurez les paramètres de base.

3. Configuration de la sécurité :

- Activez le chiffrement pour les données stockées.

- Configurez des sauvegardes régulières et des politiques de rétention.

4. Configuration du partage de fichiers :

- Configurez les utilisateurs et les groupes.

- Définissez les autorisations de partage de fichiers et configurez les liens partageables.

**FileZilla Server :**

1. Configuration de la machine virtuelle :

- Créez une machine virtuelle avec les spécifications appropriées.

- Installez un système d'exploitation pris en charge (Windows Server, par exemple).

2. Installation de FileZilla Server :

- Téléchargez et installez FileZilla Server à partir du site officiel.

- Lancez l'assistant d'installation et suivez les étapes.

3. Configuration de la sécurité :

- Configurez les paramètres de sécurité, notamment les certificats SSL/TLS pour le chiffrement des connexions.

- Mettez en place des utilisateurs et des groupes avec des permissions spécifiques.

4. Configuration du partage de fichiers :

- Créez des répertoires partagés avec des autorisations appropriées.

- Définissez les utilisateurs autorisés à accéder à ces répertoires.