**Etude des Besoins – Application Interne**

1. **Identification des Parties Prenantes**

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

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 : odyscomp01p*
* *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 et client*

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

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

* *Données Clients :*

*Informations sur les clients, y compris les coordonnées, les historiques d'achat, les préférences, etc.*

* *Données Produits/Services :*

*Informations sur les produits ou services proposés, y compris les descriptions, les tarifs, les niveaux de stock, etc.*

* *Données Financières :*

*Informations financières liées aux transactions commerciales, aux factures, aux paiements, aux relevés, etc.*

* *Données des Employés :*

*Informations sur les employés de l'entreprise, y compris les données personnelles, les rôles, les permissions d'accès, etc.*

* *Données de Commandes :*

*Informations sur les commandes passées par les clients, les statuts de livraison, les confirmations de commande, etc.*

* *Données Marketing :*

*Informations sur les campagnes marketing, les résultats, les analyses, etc.*

* *Données de Stock :*

*Informations sur les niveaux de stock, les mouvements de stock, les réapprovisionnements, etc.*

* *Données de Facturation :*

*Informations liées à la facturation des produits ou services fournis.*

* *Données de Rapports et Analyses :*

*Rapports générés par l'application pour suivre les performances commerciales, les tendances, etc.*

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

*Utilisation de mécanismes de vérification d'intégrité pour s'assurer de la fiabilité des données.*

*Mises à jour régulières du logiciel pour corriger les vulnérabilités et garantir la sécurité.*

*Surveillance continue des logs d'erreurs pour détecter toute activité suspecte.*

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

*Quelles informations sont considérées comme sensibles ou confidentielles ?*

*Données Clients, Données Produits/Services, Données Financières, Données des Employés, Données de Commandes, Données Marketing, Données de Stock, Données de Facturation, Données de Rapports et Analyses, Données de Configuration et Fichiers Source de l'Application.*

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

*Chiffrement des communications avec le serveur de l'application commerciale.*

*Gestion sécurisée des informations d'authentification des utilisateurs et des données sensibles.*

*Mise en place de politiques de confidentialité pour restreindre l'accès aux informations sensibles.*

***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 : odyscomp01p
* Réseaux : 001-int-prd-odys
* *Financières :* **Petite Entreprise (10-50 employés) :**
  + Installation initiale de l'application : Entre 10 000 et 50 000 euros.
  + Coûts annuels de maintenance : Entre 5 000 et 15 000 euros.
* **Entreprise de Taille Moyenne (50-500 employés) :**
  + Installation initiale de l'application : Entre 50 000 et 200 000 euros.
  + Coûts annuels de maintenance : Entre 20 000 et 50 000 euros.
* **Grande Entreprise (500+ employés) :**
  + Installation initiale de l'application : Plus de 200 000 euros.
  + Coûts annuels de maintenance : Plus de 50 000 euros.

1. **Conformité Réglementaire**

*Consentement et Finalité*

* *Obtenez le consentement clair des personnes pour collecter et traiter leurs données. Assurez-vous que la collecte de données est limitée aux finalités spécifiques pour lesquelles le consentement a été donné.*

*Minimisation des données*

* *Collectez et traitez uniquement les données nécessaires à la finalité spécifique pour laquelle elles sont traitées. Limitez la quantité de données collectées au strict nécessaire.*

*Exactitude des données*

* *Assurez-vous que les données personnelles sont exactes et, si nécessaire, maintenez-les à jour. Prenez des mesures pour rectifier les données inexactes ou incomplètes.*

*Sécurité des données*

* *Mettez en place des mesures de sécurité appropriées pour protéger les données personnelles contre tout accès non autorisé, divulgation, altération ou destruction.*

*Droit à l'information*

* *Informez les personnes concernées sur la manière dont leurs données sont collectées, utilisées et traitées. Fournissez des informations transparentes et compréhensibles sur la politique de confidentialité de votre application.*

*Droit d'accès et de rectification*

* *Permettez aux personnes concernées d'accéder à leurs données personnelles et de les rectifier si elles sont inexactes.*

*Limitation de la conservation*

* *Déterminez des périodes de conservation appropriées pour les données personnelles et supprimez-les lorsque ces périodes expirent, sauf si une justification légale pour la conservation existe.*

*Responsabilité*

* *Mettez en place des processus internes pour démontrer la conformité au RGPD. Cela inclut la tenue de registres, la réalisation d'évaluations d'impact sur la vie privée si nécessaire, et la collaboration avec les autorités de contrôle.*

*Transferts internationaux de données*

* *Si vos serveurs sont situés en dehors de l'UE, assurez-vous que des mécanismes juridiques appropriés, tels que les clauses contractuelles types, sont en place pour garantir un niveau adéquat de protection des données.*

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

**Installation de Microsoft Azure Active Directory :**

1. Accès au portail Azure : Connectez-vous au portail Azure avec vos identifiants Microsoft.

2. Création d'un service Azure Active Directory : Suivez les instructions pour créer un nouvel annuaire ou utiliser un annuaire existant.

3. Ajout d'utilisateurs et de groupes : Accédez à la section "Utilisateurs" pour ajouter des comptes utilisateurs et des groupes selon les besoins.

4. Attribution de rôles et de privilèges : Configurez les rôles et les permissions pour les utilisateurs et groupes créés.

**Installation de MySQL Enterprise Edition :**

1. Téléchargement de MySQL : Accédez au site de téléchargement de MySQL, choisissez la version adaptée à votre système d'exploitation et téléchargez l'installeur.

2. Installation de MySQL Server : Exécutez l'installeur téléchargé, suivez les étapes pour installer MySQL Server, définissez le mot de passe root et configurez les options de sécurité.

3. Configuration initiale : Accédez à l'interface d'administration de MySQL pour configurer les bases de données, les utilisateurs et les autorisations.

**Déploiement de Palo Alto Networks Firewall :**

1. Téléchargement de l'image du pare-feu : Connectez-vous au portail de support de Palo Alto Networks, téléchargez l'image du système d'exploitation adaptée à votre modèle de pare-feu.

2. Création d'une machine virtuelle : Utilisez votre plateforme de virtualisation pour créer une nouvelle machine virtuelle et importez l'image téléchargée.

3. Configuration initiale du pare-feu : À la première mise en marche, configurez les paramètres de base du pare-feu (adresses IP, zones de sécurité, interfaces, etc.).

4. Configuration des règles de sécurité : Utilisez l'interface de gestion du pare-feu pour définir les politiques de sécurité, les règles de filtrage, etc.