**Etude des Besoins - Web**

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 et clients.

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 : odyswww01p ; odyswww02p*
* *Réseaux : 001-int-prd-odys ; 008-ext-dmz-odys*
* *Données : Configuration, Bases de Données.*

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

*Perte d’argent pour 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 ?*

*Les données de configuration doivent être protégées.*

*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.*

*Mises à jour régulières et surveillance continue des performances pour détecter tout comportement anormal.*

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

*Quelles informations sont considérées comme sensibles ou confidentielles ?*

*Fichiers HTML, CSS, JavaScript, Photos, Vidéos, Fichiers Audios et Données de Configuration et de Paramétrage.*

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

*Utilisation de connexions sécurisées (HTTPS) pour chiffrer les données transitant entre le serveur et les clients.*

***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 et du site (ex : Statistiques sur l'utilisation du site)*

*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 Informatique*
* Serveurs : odyswww01p ; odyswww02p
* Réseaux : 001-int-prd-odys ; 008-ext-dmz-odys
* *Financières :* 
  + **Petite entreprise :** Serveur virtuel (VPS) ou hébergement partagé. Fourchette de prix : 10 $ à 200 $ par mois, selon les besoins en ressources.
  + **Entreprise de taille moyenne :** VPS ou serveur dédié avec des configurations plus robustes. Peut nécessiter des services cloud supplémentaires. Fourchette de prix : 50 $ à 500 $ par mois, en fonction des spécifications.
  + **Grande entreprise** : Serveurs dédiés, services cloud évolutifs, équilibrage de charge, etc. Possiblement des solutions d'entreprise personnalisées. Fourchette de prix : 200 $ à plusieurs milliers de dollars par mois, en fonction de la complexité des exigences.

1. **Conformité Réglementaire**

*Consentement*

* + *Obtenez le consentement des utilisateurs avant de collecter et de traiter leurs données personnelles. Le consentement doit être donné de manière libre, spécifique, éclairée et univoque.*

*Finalité du traitement*

* + *Les données personnelles collectées via le serveur web ne doivent être utilisées que dans le cadre des finalités pour lesquelles elles ont été collectées. Informez les utilisateurs de manière transparente sur ces finalités.*

*Minimisation des données*

* + *Limitez la collecte et le traitement des données personnelles au strict nécessaire pour atteindre les objectifs définis. Évitez la collecte excessive d'informations inutiles.*

*Exactitude des données*

* + *Mettez en place des procédures pour garantir que les données personnelles collectées et traitées par le serveur web sont exactes et tenues à jour.*

*Durée de conservation*

* + *Définissez des périodes de conservation appropriées pour les données personnelles stockées sur le serveur web et supprimez-les une fois qu'elles ne sont plus nécessaires.*

*Sécurité*

* + *Mettez en place des mesures de sécurité appropriées pour protéger les données personnelles stockées sur le serveur web. Utilisez des protocoles sécurisés tels que HTTPS et chiffrez les données sensibles.*

*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.*

*Notification des violations de données*

* + *En cas de violation de données personnelles entraînant un risque élevé pour les droits et libertés des personnes, notifiez cette violation aux autorités de contrôle et, dans certains cas, aux personnes concernées.*

*Traçabilité*

* + *Maintenez des registres détaillés des activités de traitement des données réalisées par le serveur web pour pouvoir démontrer la conformité en cas de besoin.*

*Responsabilité*

* + *Adoptez une approche proactive en matière de protection des données et démontrez votre conformité aux principes du RGPD. Cela peut inclure la nomination d'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.*

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

**Installation de Nginx (Serveur Web) :**

1. Prérequis :

- Une machine virtuelle avec un système d'exploitation compatible (comme Ubuntu, CentOS, etc.).

2. Installation de Nginx :

- Sous Ubuntu, ouvrez un terminal et exécutez :

sudo apt update

sudo apt install nginx

- Sous CentOS, utilisez :

sudo yum install epel-release

sudo yum install nginx

3. Configuration de Nginx :

- Les fichiers de configuration principaux sont généralement situés dans `/etc/nginx`.

- Placez vos fichiers de site web dans le dossier `/var/www/html`.

- Assurez-vous de configurer les fichiers de sites virtuels (`/etc/nginx/sites-available` et `/etc/nginx/sites-enabled`) selon vos besoins.

**Configuration de Let's Encrypt pour les certificats SSL/TLS :**

1. Installation de Certbot (outil Let's Encrypt) :

- Assurez-vous d'avoir Nginx en cours d'exécution.

- Installez Certbot :

sudo apt-get install certbot python3-certbot-nginx (pour Ubuntu)

sudo yum install certbot python3-certbot-nginx (pour CentOS)

2. Génération des certificats SSL/TLS :

- Utilisez Certbot pour obtenir et installer automatiquement les certificats :

sudo certbot --nginx -d votredomaine.com

**Installation de MySQL ou PostgreSQL (Gestion de la Base de Données) :**

1. Installation de MySQL ou PostgreSQL :

- Sous Ubuntu, pour MySQL :

sudo apt-get update

sudo apt-get install mysql-server

- Pour PostgreSQL :

sudo apt-get update

sudo apt-get install postgresql postgresql-contrib

2. Configuration et sécurisation : Après l'installation, suivez les instructions pour configurer les mots de passe et les autorisations d'accès à la base de données.

**Déploiement d'ELK Stack (Surveillance et Logs) :**

1. Installation d'ELK Stack :

- Pour Elasticsearch, Logstash et Kibana, vous pouvez suivre les instructions spécifiques à chaque composant en téléchargeant et en installant les paquets depuis les sites officiels.

2. Configuration :

- Après l'installation, configurez chaque composant pour qu'il fonctionne ensemble.

- Elasticsearch : Configurez les index, les paramètres de sécurité et les rôles.

- Logstash : Configurez les pipelines pour collecter, filtrer et acheminer les logs vers Elasticsearch.

- Kibana : Connectez Kibana à Elasticsearch et configurez les tableaux de bord pour visualiser les données.