**Etude des Besoins - Mail**

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 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 :* *odyssmp01p ; odyssmp02p*
* *Réseaux :* *001-int-prd-odys ; 008-ext-dmz-odys*
* *Données : Informations Clients, Bases de Données.*

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

*Aucunes communications entre l’entreprise et les clients et dans l’entreprise entre employés*

***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 ?*

*E-mails reçus et stockés par les utilisateurs, Éléments envoyés par les utilisateurs, Éléments brouillons par les utilisateurs, Éléments supprimés par les utilisateurs, Répertoires d'adresse, Fichiers de configuration, Base de données de messagerie, Informations d'authentification* *des utilisateurs lors de la connexion au serveur de messagerie.*

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

*Chiffrement des communications avec le serveur de messagerie (TLS/SSL).*

*Mise en place de politiques de confidentialité pour restreindre l'accès aux e-mails 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 du serveur de messagerie, y compris les connexions, les envois et les erreurs. Utilisation de mécanismes de hachage pour garantir l'intégrité de l’historique.*

*Mise en œuvre d'audits réguliers pour vérifier la conformité aux politiques de sécurité.*

*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** |
| 03 - Fort | 04 - Majeur | 04 - Majeur | 04 - Majeur | 03 - Stratégique |

1. **Évaluation des Ressources**

Voici les ressources disponibles :

* *Equipe Cybersécurité*
* Serveurs : odyssmp01p ; odyssmp02p
* Réseaux : 001-int-prd-odys ; 008-ext-dmz-odys
* *Financières :* **Petite Entreprise (10-50 employés) :**

1. **Serveur de messagerie :**
   * Installation initiale : Entre 5 000 et 10 000 euros.
   * Coûts annuels de maintenance et de support : Entre 2 000 et 4 000 euros.
2. **Application mail :**
   * Abonnement annuel : Entre 2 000 et 10 000 euros.
3. **Microsoft Exchange :**
   * Licences annuelles ou perpétuelles : Entre 2 000 et 10 000 euros.

**Entreprise de Taille Moyenne (50-500 employés) :**

1. **Serveur de messagerie :**
   * Installation initiale : Entre 10 000 et 20 000 euros.
   * Coûts annuels de maintenance et de support : Entre 4 000 et 8 000 euros.
2. **Application mail :**
   * Abonnement annuel : Entre 10 000 et 50 000 euros.
3. **Microsoft Exchange :**
   * Licences annuelles ou perpétuelles : Entre 10 000 et 50 000 euros.

**Grande Entreprise (500+ employés) :**

1. **Serveur de messagerie :**
   * Installation initiale : Plus de 20 000 euros.
   * Coûts annuels de maintenance et de support : Plus de 8 000 euros.
2. **Application mail :**
   * Abonnement annuel : Entre 50 000 et 200 000 euros.
3. **Microsoft Exchange :**
   * Licences annuelles ou perpétuelles : Entre 50 000 et 200 000 euros
4. **Conformité Réglementaire**
5. *Consentement : Si votre serveur web collecte des données personnelles, assurez-vous d'obtenir le consentement explicite des utilisateurs avant de traiter ces données. Le consentement doit être libre, spécifique, éclairé et univoque.*
6. *Finalité du traitement : Les données personnelles collectées via le serveur web ne doivent être utilisées que pour des finalités spécifiques et légitimes. Informez clairement les utilisateurs de ces finalités.*
7. *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.*
8. *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.*
9. *Durée de conservation : Définissez des périodes de conservation appropriées pour les données personnelles collectées et supprimez-les lorsque ces périodes expirent ou lorsque les données ne sont plus nécessaires.*
10. *Sécurité : Assurez-vous que le serveur web et les données qu'il traite sont sécurisés. Cela implique des mesures telles que le chiffrement des données, la gestion des accès, et la protection contre les vulnérabilités.*
11. *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.*
12. *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.*
13. *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.*
14. *Responsabilité : Assurez-vous d'adopter une approche proactive en matière de protection des données et démontrez votre conformité aux principes du RGPD.*
15. **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.