Table des matières

Mesures de sécurité à appliquer pour un serveur d'hébergement :

Afin de respecter la confidentialité des données des utilisateurs de notre hébergeur, nous avons optés pour certaines normes de sécurité à appliquer.

Dans un premier temps, nous souhaitons mettre en place un pare-feu, afin de filtrer le trafic réseau non autorisé.

Nous devrons mettre à jour notre hébergeur de manière très régulière afin d'avoir les correctifs de sécurité les plus récents. De même pour ce qui est sauvegardes.

Nous opterons pour une authentification à deux facteurs et auront recours à des clés SSH plutôt que de simples mots de passe. En effet, les clés SSH garantiront une forte authentification, en protégeant contre les attaques par force brute.

Nous mettrons en place des outils de surveillance afin de détecter et réagir rapidement aux activités suspectes. Les systèmes de préventions d'intrusion (IDS) vont venir bloquer toute tentatives d'intrusion et activités malveillantes sur le réseau ou sur les serveurs.

Nous souhaitons mettre en place un système de chiffrement de données afin de protéger les données sensibles en transit et au repos.

Nous limiterons les accès aux ressources du serveur uniquement aux utilisateurs autorisés et suivront les principes du moindre privilégié.

Nous garantirons la sécurité physique du serveur contre l'accès non autorisé, en le maintenant dans un emplacement sécurité tel que dans une salle dans une salle des serveurs.

Nous devrons mettre en place un protocole TLS (https), un VPN et un SFTP. En combinant ces derniers, la sécurité de transfert des fichiers sera assurée. Notre hébergeur web pourra mieux protéger les données clients contre les interceptions et accès non autorisés. Cela va ainsi renforcer la confiance des utilisateurs dans la sécurité de leurs données. Nous utiliserons le VPN OpenVPN.

Nous finirons par instaurer une charte à la vue des clients, afin de les sensibiliser à la sécurité des systèmes et à leurs responsabilités en matière de sécurité.

Politique de sécurité :

1. Objectif :

Notre objectif primaire est d'assurer la sécurité des données clients, des serveurs et des réseaux afin de garantir la confidentialité, l'intégrité et la disponibilité des services d'hébergement web. Pour se faire, nous allons mettre en œuvre une combinaison de mesures de sécurité robustes, telles que le déploiement de pare-feu avancés, la configuration de certificats SSL/TLS pour le chiffrement des communications, la mise en place de politiques strictes de contrôle d'accès, ainsi que la surveillance continue des activités réseau et système.

2. Accès et authentification :

Nous utiliserons des méthodes d'authentification forte pour accéder aux systèmes et aux données sensibles et limiterons l'accès aux serveurs uniquement aux employés autorisés en fonction de leurs besoins. Pour se faire, nous opterons pour des méthodes d'authentification robustes et restreindrons l'accès aux serveurs uniquement aux employés autorisés en fonction de leurs besoins.

3. Gestion des mises à jour :

Nous appliquerons régulièrement les correctifs de sécurité et les mises à jour logicielles sur les serveurs pour combler les vulnérabilités.

4. Surveillance et détection :

Nous mettrons en place des outils de surveillance afin de détecter les activités suspectes et toute tentatives d'intrusion. Il faudra pour cela, réagir rapidement aux alertes de sécurité et enquêter sur les incidents potentiels.

En cas de détection d'une activité anormale, des alertes de sécurité seront automatiquement déclenchées, et notre équipe de sécurité interviendra immédiatement pour enquêter sur l'incident et prendre des mesures correctives afin de protéger nos systèmes et nos données contre toute menace potentielle.

5. Sécurité réseau :

Nous configurerons et maintiendrons un pare-feu afin de filtrer le trafic réseau non autorisé.
Afin de protéger les données en transit entre les serveurs et les clients, nous utiliserons le chiffrement. Cela va renforcer la sécurité de notre réseau tout en garantissant la confidentialité des informations échangées.

6. Sauvegardes :

Nous effectuerons des sauvegardes régulières des données clients afin de minimiser les pertes en cas de sinistre ou de compromission. Nous utiliserons des solutions fiables tout en testant régulièrement la restauration des sauvegardes afin de garantir leur efficacité.

Nous mettrons en œuvre des sauvegardes différentielles. Cela permettra de sauvegarder toutes les données modifiées depuis la dernière sauvegarde complète.

7. Gestion des incidents :

Afin de répondre aux violations de sécurité et rétablir les services rapidement de manière efficace, nous établirons des procédures de gestion des incidents. Ces procédures comprennent des plans d'action détaillés, une équipe d'intervention formée et des processus de communication clairs.

8. Conformité réglementaire :

Nous devrons être conforme aux lois et réglementations en matière de protection des données et de confidentialité des informations. Pour cela, nous mettrons en place des procédures de sécurité conformes aux normes telles que le RGPD (Règlement Général sur la Protection des Données) et nous nous assurerons que nos pratiques de collecte, de stockage et de traitement des données respectent les principes de confidentialité et de protection des données personnelles.