Rapport d'évaluation de la vulnérabilité

26 Février 2026

Description du système

Le cœur de l'analyse repose sur un serveur haute performance tournant sous **Linux**. Voici ses caractéristiques principales :

- **Capacité :** Équipé de 128 Go de RAM pour traiter de gros volumes de données.
- **Technologie :** Héberge une base de données **MySQL**.
- **Sécurité réseau :** Utilise des connexions chiffrées **SSL/TLS** et communique via des adresses IPv4 stables.

Portée

L'audit se concentre spécifiquement sur les **contrôles d'accès** du système sur une période de trois mois. Pour garantir une analyse rigoureuse et conforme aux standards de l'industrie, j'ai utilisé le cadre de référence **NIST SP 800-30 Rév. 1** pour orienter l'évaluation des risques.

But

Ce serveur est un système centralisé qui stocke des informations sensibles : données clients, résultats de campagnes et analyses marketing. Comme ces données sont utilisées quotidiennement pour personnaliser nos actions commerciales, leur intégrité et leur confidentialité sont vitales pour l'organisation. Ma mission est donc de m'assurer qu'aucune vulnérabilité ne permet un accès non autorisé à ce patrimoine numérique.

L'évaluation des risques

Source de la menace	Événement menaçant	Probabilité	Gravité	Risque
Hacker	*Obtenir des informations sensibles par exfiltration*	*3*	*3*	*9*

Employé	*Perturber les opérations critiques*	*2*	*3*	*6*
Client	*Modifier/Supprimer des informations critiques*	*1*	*3*	*3*

Approche

L'analyse des risques a été menée en évaluant la probabilité d'incidents par rapport aux autorisations d'accès actuellement ouvertes. Chaque menace potentielle a été pondérée selon son impact réel sur les opérations quotidiennes de l'organisation. Cette méthode permet de prioriser les interventions là où le risque métier est le plus élevé.

Stratégie de remédiation

Pour corriger les failles identifiées, j'ai défini une stratégie multicouche basée sur le contrôle strict des accès et la protection des flux :

- **Renforcement de l'Accès :** Mise en place de politiques de mots de passe robustes et déploiement de l'**authentification multifacteur (MFA)** pour limiter les privilèges.
- **Contrôle basé sur les Rôles (RBAC) :** Restructuration des accès pour s'assurer que chaque utilisateur ne dispose que des droits strictement nécessaires à sa fonction.
- **Sécurisation des Flux :** Migration systématique du protocole SSL vers le **TLS** pour garantir un chiffrement optimal des données en transit.
- **Protection Réseau :** Restriction stricte des accès à la base de données aux seules adresses IP des bureaux de l'entreprise, bloquant ainsi toute tentative de connexion non autorisée depuis l'Internet public.