Rapport d'Évaluation des Vulnérabilités

Objectif

Le serveur de base de données est essentiel aux activités de prospection commerciale mondiale de l'entreprise. Sécuriser les données est impératif pour protéger les informations clients contre des accès non autorisés, prévenir des violations RGPD, et maintenir la réputation de l'entreprise. Si le serveur était désactivé, les activités de vente s'arrêteraient immédiatement, entraînant des pertes financières significatives et une érosion de la confiance des clients. Cette analyse vise à identifier les risques critiques liés à l'exposition publique du serveur et à prioriser des mesures correctives urgentes.

Évaluation des Risques

Source de menace	Événement de menace	Probabilité	Gravité	Risque
Hacker / APT	Obtenir des informations sensibles via exfiltration	3	3	**9**
Concurrent	Altérer/Supprimer des informations critiques	2	3	**6**
Logiciel malveillant	Installer des renifleurs réseaux persistants	3	3	**9**

Approche

Les trois menaces sélectionnées (Hacker/APT, Concurrent, Logiciel malveillant) reflètent l'exposition critique d'un serveur public sans contrôles d'accès stricts. Le risque d'**exfiltration de données** (score 9) est prioritaire car le serveur héberge des données clients accessibles mondialement. La menace de **sabotage par un concurrent** (score 6) a une probabilité modérée mais un impact commercial catastrophique. L'installation de **renifleurs réseau** (score 9) est hautement probable via des vulnérabilités non patchées, menaçant la confidentialité des échanges.

Remédiation

1. **Contrôles d'accès** :

   -Appliquer le **principe du moindre privilège** et l'**authentification multifacteur (MFA)** pour limiter les accès distants.

   -Isoler le serveur dans un réseau privé (VPN obligatoire).

2. **Défense en profondeur** :

   -Déployer un **pare-feu applicatif (WAF)** et un **système de détection d'intrusion (IDS)** pour bloquer les requêtes malveillantes.

   -Chiffrer les données **en transit (TLS 1.3)** et **au repos**.

3. **Cadre AAA** :

   -Implémenter une journalisation centralisée des accès (**comptabilité**) et des revues mensuelles des permissions (**autorisation**).