Rapport d'évaluation de la vulnérabilité

1St janvier 20XX

Description du système

Le matériel du serveur se compose d'un puissant processeur CPU et de 128 Go de mémoire. Il fonctionne sur la dernière version du système d'exploitation Linux et héberge un système de gestion de base de données MySQL. Il est configuré avec une connexion réseau stable utilisant des adresses IPv4 et interagit avec d'autres serveurs du réseau. Les mesures de sécurité incluent des connexions cryptées SSL/TLS.

Portée

La portée de cette évaluation de vulnérabilité concerne les contrôles d'accès actuels du système. L'évaluation couvrira une période de trois mois, du juin 20XX au août 20XX. NIST SP 800-30 Rév. 1 sert à orienter l'analyse des risques du système d'information.

But

L'entreprise ayant des employés à des sites distants, a besoin d'une base de données pour permettre aux différents travailleurs d'accéder aux données nécessaire l'exécution de leur tâches. En cas de désactivation les employés distants ne pourraient pas atteindre le système . Le serveur est utilisé pour stocker les données client, de campagne et analytiques qui peuvent ensuite être analysées pour suivre les performances et personnaliser les efforts marketing. Ainsi si le public a accès à ce base de donnée, ils peuvent accéder à des PII de clients pour potentiellement l'utiliser à mauvais escient.

L'évaluation des risques

Source de menace	Événement de menace	Probabilité	Gravité	Risque

Concurrent	*Obtenir des informations par exfiltration*	*1*	*3*	*3*
Pirate informatique	*Mener Des attaques DOS*	*3*	*3*	*6*
Alimentation défectueuse	*Perturber les opérations critiques*	*1*	*3*	*3*

Approche

Les risques mesurés ont pris en compte les procédures de stockage et de gestion des données de l'entreprise. Les sources et événements potentiels de menaces ont été déterminés en utilisant la probabilité d'un incident de sécurité compte tenu des autorisations d'accès ouvert au système d'information. La gravité des incidents potentiels a été mise en balance avec leur impact sur les besoins opérationnels quotidiens.

Stratégie de remédiation

Une mise en œuvre d'authentification, autorisation, comptabilité avec le principe de moindre privilège permettra aux seuls employés légitimes et qui ont besoin de l'accès pour effectuer leur tâche d'accéder à la base de données. L'utilisation d'une MFA ajoutée d'une politique de mot de passe forte augmentera une couche défense et permettra d'améliorer la posture de sécurité de la base de données.Une infrastructure de clé publique pourra permettre de publique permettra de remédier à l'exfiltration des données. Il faut aussi la mise en place d'une maintenance régulière pour pallier les risques d'une alimentation défectueuse