Vulnerability Assessment Report

1st January 20XX

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

El servidor de base de datos es un activo crítico que almacena información valiosa sobre clientes potenciales necesaria para las operaciones diarias de la empresa de comercio electrónico. Proteger estos datos es fundamental para mantener la confianza del cliente y asegurar la ventaja competitiva de la empresa. Por lo tanto, el propósito de esta evaluación es identificar las vulnerabilidades de este servidor accesible al público y comunicar los riesgos potenciales para prevenir ataques que pudieran comprometer la economía y las operaciones del negocio.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker/Outsider	DoS (Denegación de servicios)	3	3	9
Privileged user/Admin	Alterar/Eliminar información crítica	2	3	6

Approach

El proceso de selección de riesgos se basó en una evaluación cualitativa que prioriza los tres pilares de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad (CIA). Esta aproximación asegura que los riesgos evaluados sean significativos y representen un espectro completo de amenazas para el negocio. La selección de fuentes de amenaza consideró el riesgo del Competito y el Hacker/Outsider por la naturaleza públicamente accesible del servidor. Finalmente, se incluyó el Privileged User para abordar el riesgo interno y el potencial de alto impacto en la Integridad y Confidencialidad de los datos.

Las puntuaciones de Probabilidad (Likelihood) y Gravedad (Severity) se derivaron siguiendo las directrices de la guía NIST SP 800-30 Rev. 1, utilizando el juicio experto para una evaluación cualitativa. La Probabilidad se evaluó considerando la exposición pública del servidor, los eventos de amenaza externa (Competitor, DoS) recibieron una puntuación Alta (3) por su mayor frecuencia en servidores accesibles. La Gravedad de todos los eventos se calificó como Alta(3), ya que la interrupción, eliminación o exfiltración de los datos de la base de clientes causaría un impacto catastrófico y multifacético en la economía y la reuptación de la empresa de comercio electrónico.

Remediation Strategy

La estrategia de remediación se centra en implementar una Defensa en Profundidad para mitigar los riesgos de alto impacto. Para contrarrestar la alta probabilidad de ataques externos, se deben implementar controles de red robustos contra Ataques DoS (como servicios de mitigación en la nube) y la restricción de acceso mediante listas de IP (allow-listing). La Autenticación Multifactor (MFA) y el Principio del Menor Privilegio son esenciales para proteger las credenciales de los usuarios privilegiados y reducir el riesgo de Exfiltraco;on y Alteración de datos. Finalmente, una política de Backups automatizados y probados debe establecerse como el control final para asegurar la Integridad y Disponibilidad de los datos críticos de clientes.