Vulnerability Assessment Report

20st Diciembre 2025

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

The server is used to store customer, campaign, and analytic data that can later be analyzed to track performance and personalize marketing efforts. In these cases, it is important to have a private database, regardless of whether they have been active for three years (a short time in the organization). This is because the database must be exclusively private within the organization. If the database is public, it can create problems for an attack or manipulation of the respective information.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	*Obtain sensitive information via unethical hacking*	*3*	*3*	*9*
Employee	*Obtain or delete sensitive information via research*	*2*	*3*	*6*

Approach

Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system This approach was developed by analyzing the causes and importance of databases within an organization. Since databases are required to be private, the fact that they are currently public creates an inevitable situation where a hacker is more likely to extract significantly more information than if they were private. Therefore, hacks or malicious employees gaining access to this information are quite probable, making it essential to consider the points in the table.

Remediation Strategy

The results should contribute to system security through the use of reliable security techniques. It is important to maintain restrictions on who accesses people's personal information; not everyone should have access to such data.
It is important to use multi-factor authentication as well as the Principle of Least Privilege, using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges.