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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
  The database server is used to store all the information and data for all the business operations systematically. The whole operation of the business depends on the data stored inside the database.

- *Why is it important for the business to secure the data on the server?*
  The data may contain trade secrets, user PII and SPII and other confidential information that should not be accessible to anyone other than the authorized individuals. It could be devastating for the business if those confidential data is leaked or held captive due to some ransomware attack.

- *How might the server impact the business if it were disabled?*
  The daily task of the business will be hampered, and the business will also lose its reputation. Clients might also not be able to perform their task, which may lead to a financial loss of the business as well as the business may have to pay some hefty fines.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Employees	*Disgrumbled employees may leak or sell sensitive information or employees may fall for social engineering attacks*	*2*	*3*	*6*
Non configured Firewalls, IDS and IPS	*Weaken the entire security of the business*	*2*	*3*	*6*

Approach

It is not so likely that the competitors that competitors will steal our sensitive information but there is a possibility and if it happens it will be devastating to the business as the trade secrets and other information can be used to hamper our business.

Not the 100% of the employees may be technically sound, and not everyone may have good intentions. Technically naive employees may be easily be compromised by social engineering attacks, and some employees may sell sensitive information for profit.

Unconfigured or poorly configured firewalls and IPS may put the whole business at risk as it will be easily bypassed by the adversary and perform all sorts of attacks to harm the business operations.

Remediation Strategy

Information should be limited in need to know basis, employees would only be given access that is required to them to perform their job, MFA should be implemented strictly, employees would be provided with proper knowledge about social engineering attacks, firewalls , IPS and IDS should be properly configured.