**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](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Purpose

As cybersecurity analysts, we should ask ourselves the following questions, considering the context of the organization we are currently analyzing.

* ***How is the database server valuable to the business?***

*The server is very important to the organization because it receives many external connections from employees, and using the functionalities and information from the server is fundamental.*

* ***Why is it important for the business to secure the data on the server?***

*It's important that data is well-protected. The server receives many requests from employees throughout the day, so it's fundamental that data is not leaked or exploited by cybercriminals.*

* ***How might the server impact the business if it were disabled?***

*The most immediate impact would be the unavailability of all services, applications, and data hosted on that server.*

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration.* | *1* | *3* | *3* |
| *Outsider* | ***Attack the server*** *by looking for errors in* ***security configurations*** *and* ***unauthorized accesses*** *to obtain information.*  *Alter / Del critical information* | *3* | *3* | *9* |
| *Software* | *Server Up to Date with the latest security updates.*  *Obfuscate future attacks* | *2* | *2* | *4* |

# Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

# Remediation Strategy

**Immediate Access Restriction:** **Firewall** to limit access to only authorized IP addresses (e.g., VPNs used by remote employees or specific company network ranges).

**Secure Remote Access Implementation:** For remote employees, we need to ensure they access the database through a **Virtual Private Network (VPN)**. This encrypts their connection and routes it through a secure tunnel, making it much harder for unauthorized parties to intercept data.

* Implementing **strong, unique passwords** and enforcing regular password changes.
* Considering **multi-factor authentication (MFA)** for all database access.
* Implementing the **principle of least privilege**, ensuring employees only have access to the specific data and functions necessary for their roles.

We need to conduct a thorough **vulnerability scan and penetration test** on the database server to identify any other misconfigurations, unpatched software, or hidden vulnerabilities.

We must ensure that comprehensive logging is enabled for all database activities, and we need to establish **real-time monitoring and alerting** for suspicious access patterns or activities. This will help detect and respond to any potential breaches quickly.

We need to verify that regular, secure backups of the database are being performed and that a robust disaster recovery plan is in place in case of data loss or corruption.