**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

**DB server is valuable for many reasons:**

* **Massive business case because they have a list of prospects or potential customers**
* **Could damage their reputation if data is leaked**

**It is essential for businesses to secure the data on the server because exposure of the data could potentially violate data privacy laws. If the server were disabled, the data would be held at ransom and the business would no longer have access to customers and prospects.**

# Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Employee* | *Perform reconnaissance and surveillance of organization* | *2* | *3* | *6* |
| *Business Partner* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Advanced Persistent Threat (APT)* | *Alter/Delete Critical information* | *1* | *3* | *3* |

# Approach

The 3 specific threat sources are employee(s), business partner(s), and Advanced Persistent Threats (APTs) because they are part of various risk groups and are a threat for many different reasons. Employees are a major threat because they have internal knowledge and access to company data and they are the biggest threat to a company’s security because of that. A business partner may receive information by employees via exfiltration which they could reveal on social media or pose a threat in other ways as well. APTs are external threats that when they get into a company’s system, they can alter & delete critical data.

# Remediation Strategy

There are 3 remediation and/or risk mitigation methods to use: they are the AAA framework, Principle of Least Privilege, and Defense-in-depth strategies.

Here’s how you can implement Authentication, Authorization, and Accounting:

Authentication

* MFA: require multiple factors such as biometrics and passwords to access DB server
* Certificate-Based Authentication: Digital certificates to securely authenticate users/services
* Strong password Policies

Authorization

* Enforce Role-Based Access Control (RBAC)
* Context-Based: based on factors like Time of Day, IP address, or device used

Accounting

* Centralized Audit Logging: store logs in central, tamper-proof location using tools like SIEM
* Perform Regular Audits & Reviews: Periodically audit logs for suspicious user activities
* Real-Time Alerts: Alerts for critical events like failed login attempts or data exposure