**Vulnerability Assessment Report**

**21st September 2023**

**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 2023 to August 2023. [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**

The database server is one of our most valuable assets. The server stores all information regarding past, current, and future customers, including Personally Identifiable Information (PII), which our employees regularly request data from. This server has been open to the public ever since the company's launch three years ago. If a data breach occurs as we are now, at the very least we will be found non-compliant with at least the Payment Card Industry Data Security Standard (PCI DSS) and risk heavy fines.

**Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| Customer | Alter/Delete critical information | 1 | 3 | 3 |
| Hacker | Obtain Sensitive information via exfiltration | 3 | 3 | 9 |
| Advanced Persistent Threat (APT) | Disrupt mission-critical operations | 2 | 3 | 6 |

**Approach**Considering the state of our server, there are three threat sources and multiple events that would impact our business. The first threat source is our customers. They would be able to cause our business to be paralized by altering or deleting critical information needed for day-to-day business operations. The second threat source is the Advanced Persistent Threat (APT). They would be able to compromise the integrity of information in a way that prevents the business from carrying out critical operations. Finally, the third threat source is the hacker. They would be able to obtain sensitive information via exfiltration by installing malicious software on organizational systems to locate and aquire sensitive information.

**Remediation Strategy**Using the Authentication, Authorization, and Accounting (AAA) framework, ensure that the right user is granted access to the right resources at the right time for the right reasons. Adopting the principle of least privilege will help defend against hackers and customers by not having any one user or employee access to more than is needed. To defend against exfiltration, impliment a public key infrastructure (PKI) with asymmetric encription and digital certificates. Finally, It is highly recommended to ensure secure login credentials by using a hashing algorithm (ideally SHA-256) with salting.