**Vulnerability Assessment Report**

**26 January 2024**

**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 2024 to August 2024. [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**

Consider the following questions to help you write:

The database server is valuable to XYZ Financial Services due to the protection and storage of customer accounts, transaction processes, and information related to online

banking services provided to its clients. Protecting customer data,

ensuring regulatory compliance, and maintaining the integrity and

availability of financial services are essential to the integrity and success of the business.  In the event, that the server becomes unavailable XYZ Financial Services will be affected both on-site and remotely.

**Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Power Outages* | *Disabled servers, online services interruptions, delayed internal communication* | *2* | *3* | *3* |
| *Employee* | *Shared access with unauthorized individuals* | *2* | *3* | *3* |
| *Customer* | *Shared personal data* | *2* | *2* | *2* |

**Approach**

Risks considered the business's data storage and management methods. 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**

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.

Updates to the system hardware and software can range from a cost of $8,000 to $25,000 over 6-8 months. Given the figures, XYZ Financial Services needs to plan for a rough project estimate of $75,000 to accommodate any changes, delays, or extensions on the overall project specifications.

Lastly, security management training needs to be ongoing amongst employees and management personnel to ensure the company is utilizing and upgrading the skills and intellect of our employees consistently.

**Responsible Parties**

The teams that will be responsible include:

IT Security

Vulnerability Management Team

Security Engineering Team

Governance, Risk, and Compliance Team

Network Engineering Team

**Conclusion**

The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs. Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server are priorities. Given the figures, XYZ Financial Services needs to plan for a rough project estimate of $75,000 to accommodate any changes, delays, or extensions on the overall project specifications. Consistent and strict implementation of these upcoming updates is essential to the continued success of XYZ Financial Services.