**Vulnerability Assessment Report**

**25th of January 20, 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, network infrastructure, data storage, and other relevant areas of the system. [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**

XYZ Financial Services relies highly on the information system to conduct daily operations. The information system is responsible for managing customer accounts, processing transactions, and providing online banking services to clients. It is essential to secure customer data and financial information from all threats, internal and external, that may impact business operations. Protection of the integrity and confidentiality of customer data is vital to XYZ's reputation and operations. A breach in security can lead to the disruption of critical operations, loss of communication, and legal ramifications.

**Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| Insider | Perform reconnaissance and gather information | 1 | 3 | 2 |
| Insider | Alter/Delete critical information | 2 | 3 | 1 |
| Insider | Mishandling of critical and/or sensitive information by authorized users | 1 | 3 | 2 |
| Outsider | Conduct attacks targeting and compromising personal devices of critical employees. | 2 | 3 | 3 |
| Outsider | Disrupt mission-critical operations. | 2 | 2 | 2 |
| IT Equipment | Pervasive disk error | 1 | 2 | 1 |
| Operating system | Incorrect privilege settings | 2 | 2 | 1 |
| Operating system | Introduction of vulnerabilities into software products | 2 | 1 | 1 |
| Operating system | Spill sensitive information | 1 | 3 | 2 |
| Networking | Communications contention | 1 | 2 | 2 |
| Networking | Craft counterfeit certificates. | 2 | 3 | 3 |

**Approach**

Risks considered are 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**

XYZ Financial Services' remediation plan will discuss actions to mitigate risk associated with the identified vulnerabilities. Management will need to implement access control improvements to limit user privileges. Role-based access controls and multifactor authentication should be considered. Patch management procedures are crucial to identifying, testing, and applying updates to software, operating systems, and applications within XYZ Financials’ information technology infrastructure. Benefits of patch management include reduced attack surface, malware spread prevention, automated security fixes, vulnerability mitigation, enhanced cyberattack resistance, data protection and network security, business continuity, and regulatory compliance. Security awareness training for employees will also reduce vulnerabilities concerning employee misuse of data.