**Vulnerability Assessment Report**

**27th February 2025 \*SCENARIO LISTED AT BOTTOM\***

# **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 is used to guide the risk analysis of the information system.

# **Purpose**

The database server is a centralized computer system that is responsible for storing and managing large amounts of data. The server has multiple functions and uses. A few of these are to store customer information, details regarding the campaign, and analytic data that can later be utilized for different functions such as tracking performance or using trends to come up with more personalized marketing tactics. Ensuring the security of this system is vital because of its constant and regular usage in various marketing operations.

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Competitor* | *Utilizing some form of disruption such as a DDoS attack* | *1* | *3* | *3* |
| *Employee* | *Disruption of critical functions and operations accidentally or disgruntled employees* | *2* | *3* | *6* |
| *Hacker* | *Gain access to sensitive information via data exfiltration* | *3* | *3* | *9* |
| *Customer* | *Make modifications to critical information* | *1* | *3* | *3* |

# **Approach**

The evaluation of risks involved a thorough analysis of the business's data storage and management procedures to ensure the security and integrity of sensitive information. To identify potential threats, various sources and possible security incidents were examined, taking into account the likelihood of such occurrences based on the existing open access permissions within the information system. Furthermore, the potential severity of these incidents was assessed by measuring their possible consequences and disruptions to the organization's daily operations. This approach allowed for a balanced assessment of security vulnerabilities while maintaining the necessary accessibility for business functions.

# **Remediation Strategy**

To mitigate security risks, several measures will be implemented to strengthen authentication, access controls, encryption, and monitoring. Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) will be enforced to limit user privileges and prevent unauthorized access. Strong password policies and IP allow-listing will further restrict database access to authorized personnel. Data security will be enhanced by encrypting information both in transit with TLS and at rest to prevent unauthorized access. Remote access will require secure connections such as VPNs or SSH tunnels. Continuous security logging, regular audits, and an Intrusion Detection System (IDS) will monitor and detect suspicious activities. To reduce public exposure, the database server will be placed behind a firewall, accessible only to authorized users. A Web Application Firewall (WAF) will block malicious traffic, while DDoS protection will prevent service disruptions. Employee training on cybersecurity best practices and an incident response plan will ensure staff can identify threats and respond effectively.

These measures will significantly reduce vulnerabilities, enhance data security, and maintain system integrity while supporting business operations.

**Scenario:**

**The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability. We are tasked with completing a vulnerability assessment of the situation to communicate the potential risks to decision makers at the company. We must create a written report that explains how the vulnerable server is a risk to business operations and how it can be secured.**