**Vulnerability Assessment Report**

**System Description**

**Server Configuration**

* **Hardware:** Robust CPU processor, 256GB memory
* **Operating System:** Latest version of Ubuntu Linux
* **Database Management System:** PostgreSQL
* **Network Connection:** Stable IPv4 and IPv6 connectivity
* **Security Measures:** Utilizes SSL/TLS for encrypted connections and employs a firewall for network security.

**Scope**

The vulnerability assessment will focus on evaluating the current access controls within the system. The assessment will cover the period from June 2024 to August 2024, following the guidelines outlined in NIST SP 800-30 Rev. 1.

**Purpose**

**Importance of the Database Server to the Business**

The database server is critical for XYZ Financial Services, serving as the backbone for managing diverse financial products and services. It facilitates customer account management, transaction processing, and online banking services, making its security paramount for regulatory compliance and customer trust.

**Significance of Data Security**

Securing data on the server is imperative to safeguard sensitive financial information. Unauthorized access could lead to breaches, financial loss, and reputational damage, emphasizing the need for robust security measures.

**Impact of Server Disruption**

A disabled server could lead to severe disruptions, impacting customer services, transaction processing, and overall business operations. Such an event could result in financial losses and harm the organization's reputation.

**Risk Assessment**

| **Threat Source** | **Threat Event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| Insider Threat | Unauthorized Access | 2 | 4 | 8 |
| External Hackers | DDoS Attack | 3 | 3 | 9 |

**Approach**

The vulnerability assessment considered data storage and management methods. The likelihood of threat occurrence and potential impact were assessed against day-to-day operational needs.

**Remediation Strategy**

To mitigate identified risks, the following remediation strategies are recommended:

**1. Access Controls**

* **Implementation:** Strengthen authentication, authorization, and auditing mechanisms.
* **Details:**
  + Implement Biometric Authentication: Enhance user authentication with biometric measures.
  + Periodic Access Audits: Regularly review and audit user access to identify and address any anomalies.
* **Purpose:** Ensure only authorized and authenticated users have access to the database server, reducing the risk of unauthorized access.

**2. Data Encryption**

* **Implementation:** Enhance encryption protocols for data in motion and at rest.
* **Details:**
  + Implement AES-256 Encryption: Upgrade encryption algorithms for stronger data protection.
  + Encrypt Data at Rest: Utilize encryption to protect data stored on the server.
* **Purpose:** Improve the overall confidentiality and integrity of data, both in transit and at rest.

**3. DDoS Mitigation**

* **Implementation:** Deploy DDoS mitigation solutions.
* **Details:**
  + Collaborate with a DDoS Protection Service: Engage with a service provider to mitigate DDoS attacks effectively.
  + Implement Rate Limiting: Set limits on incoming requests to prevent overwhelming the server.
* **Purpose:** Reduce the risk of service disruption caused by DDoS attacks, ensuring uninterrupted services.

**Conclusion**

This vulnerability assessment sheds light on potential risks associated with the database server. Implementing the recommended remediation strategies will fortify XYZ Financial Services' cybersecurity posture, safeguarding customer data and ensuring the resilience of financial services. Regular assessments and proactive security measures are critical to adapting to evolving cyber threats.

Top of Form