Vulnerability Assessment of Financial Institution

Scenario:

I am a cybersecurity analyst at a local bank. The bank stores information on a remote database server. The bank has 200 employees who work remotely around the world. The employees regularly query and request data from the server. The database server setting was set open to the public 3 years ago. I noticed that keeping the database server open to the public poses a serious vulnerability to the bank.

System environment:

The system environment highlights the relevant components, architecture, and dependencies of the system being assessed. All of these parts make up the attack surface of the vulnerable info system. The bank's 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. **The access control for the database server is set open to the public.** The server is configured with a stable network connection using Ipv4 addresses and it interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Assessment Scope:

The scope specifies the focus and boundaries of the assessment. Here, the scope covers **the CIA (confidentiality, integrity, availability) of the data on the server** – not the physical security of the server or its related IT systems. The assessment will cover a period of 3 months (September 2024 to December 2024). The NIST SP 800-30 Rev.1 is used to guide the risk analysis of the information system.

Assessment Purpose:

The database server functions as a central computer system responsible for storing and overseeing critical information that are essential for business operations. The server is employed to house confidential financial info as well as customer information that includes sensitive PII information. Threat actors could purposefully or accidentally exploit vulnerabilities of the database server; for example they may alter data to negatively affect the company or intentionally steal data and damage the business. Identifying and remedying the vulnerabilities and potential threat events is important in ensuring the security of the system to protect the data from non-authorized users and ensure the safety of critical business operations.

Vulnerability Assessment

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk**
Hacker (External)	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Competitor (External)	*Utilizing technical capabilities for a denial-of-service attack*	*2*	*3*	*6*

Employee (Internal)	*Deliberately disrupt mission-critical operations (threat source compromises the integrity of information in a way that prevents the business from carrying out day-to-day operations)*	*2*	*3*	*6*

Approach

This section documents the approach used to conduct the vulnerability assessment report. It helps stakeholders understand the credibility of the report, and helps them make informed decisions. Some questions I considered for this section are:

- Is the threat relevant to the system?
- Is the threat internal or external?
- What is the threat actor's intent?
- What are the threat actors' technical capabilities?

According to the scenario, the server contains important financial and customer data. **Since the server access setting has been set open to the public,** various actors could have taken advantage of this vulnerability and participate in threat events such as obtaining sensitive information, altering/deleting critical information, and disrupting mission-critical operations. These threats pose significant business risks as they could lead to disruption in day-to-day business operations and potential fines and lawsuits stemming from failure to comply with data privacy regulations.

Threat source:

- **Hacker:** The unauthorized access threat from an external hacker emphasizes the need for robust security measures to protect sensitive information.
- **Employee**: The insider threat from an employee acknowledges the internal risk of deliberate disruptions, and it underscores the importance of internal security protocols.
- **Competitor**: The consideration of a competitor leveraging technical capabilities for a denial-of-service attack recognizes the external risk to business continuity; it emphasizes the need for proactive measures to safeguard against potential disruptions.

Limitations:

The limitations of the assessment comes from the lack of details on what kinds of data existed in the database. For example, additional details such as **data types** (e.g. customer information, internal product information, network info) and the **data security importance** (e.g. highly confidential, confidential, and public) would be helpful. Additional info on the **operational environment** of the server (e.g. temperature controls, humidity, and power supplies) would be helpful in advancing the assessment.

Remediation Strategy

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed. The questions I considered for this section are:

- Which technical, operational, or managerial controls are currently implemented to secure the system?
- Are there security controls that can reduce the risks I evaluated? What are those controls and how would they remediate the risks?
- How would the results of the assessment improve the overall security of the system?

Based on these questions, I considered the following recommendations that are realistic and achievable to ensure that risks are addressed in a timely and effective manner.

External threat: For the unauthorized access threat from external hackers and competitors, enforcing **the principle of least privilege** and **role-based access controls** would ensure that access rights are strictly limited to only those who need it to perform their work; any other access should be de-provisioned in order to minimize the potential impact of a breach.

Internal threat: In addition to role-based access controls, adopting a **defense-in-depth strategy** would add layers of protection against the insider threat; additional software measures such as anti-virus/malware/firewall/IDS/IPS should be in place to safeguard critical operations in the event of internal security lapses.

Overall threat: Instituting the use of strong passwords and **multi-factor authentication (MFA)** when accessing the database server would enhance access security. Employing a **robust AAA** (authentication, authorization, and accounting) framework by **conducting audits on access provision to the server** would establish comprehensive control over user access and mitigate the risk of deliberate disruptions. **Using** TLS instead of outdated SSL would enhance the encryption of data in communication. **IP allow-listing** to corporate offices around the world would prevent random users from connecting to the database server. Finally, **adopting PKI (public key infrastructure)** would ensure only authorized users and devices could access sensitive information and systems of the server by verifying identities via digital certificates; it would prevent exfiltration of sensitive info from the server.