## ****Name:** Ayela Israr Haqqani**

## ****Introduction****

This report provides a security assessment of the core banking system, focusing on identifying potential threats and vulnerabilities at different stages, analyzing their impact and likelihood, prioritizing them, and proposing mitigation strategies. The assessment follows a structured approach, incorporating threat modeling using IriusRisk.

## ****2.Threat Identification & Vulnerability Analysis****

The following threats and vulnerabilities are categorized based on the different stages of the banking system:

### ****2.1 Data Input Stage****

* **Threats:** Input validation flaws, phishing attacks, identity fraud, malware injection.
* **Vulnerabilities:** Lack of multi-factor authentication (MFA), inadequate input sanitization, weak password policies.

### ****2.2 Data Processing Stage****

* **Threats:** Privilege escalation, insider threats, unauthorized API access, data manipulation attacks.
* **Vulnerabilities:** Insecure APIs, weak access controls, inadequate logging and monitoring.

### ****2.3 Data Storage Stage****

* **Threats:** Data breaches, ransomware attacks, database tampering, unauthorized data access.
* **Vulnerabilities:** Lack of encryption, misconfigured database permissions, outdated software.

**2.4 Data Output Stage**

* **Threats:** Data leakage, unauthorized report access, improper log handling.
* **Vulnerabilities:** Unprotected session data, improper logging mechanisms, insecure data transmission.

**3. Risk Analysis**

Each identified threat is analyzed based on its impact and likelihood:

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat** | **Impact** | **Likelihood** | **Severity** |
| Phishing Attacks | High | High | Critical |
| Privilege Escalation | High | Medium | High |
| Ransomware Attacks | High | High | Critical |
| API Exploitation | Medium | High | High |
| Data Leakage | Medium | Medium | Moderate |

## ****4. Threat Prioritization****

Based on severity, the top-priority threats include:

1. Phishing Attacks
2. Ransomware Attacks
3. Privilege Escalation
4. API Exploitation
5. Data Leakage

## ****5. Mitigation Strategies****

### ****5.1 Technical Controls****

* Implement MFA for all user access.
* Enforce input validation to prevent injection attacks.
* Apply robust encryption (AES-256) for data storage and transmission.
* Deploy endpoint detection and response (EDR) solutions.

### ****5.2 Procedural Controls****

* Conduct regular security awareness training for employees.
* Implement strict access controls with least privilege principles.
* Regularly audit API security and apply token-based authentication.

### ****5.3 Policy-Based Controls****

* Enforce a strong password policy and periodic password changes.
* Establish a formal incident response plan for security breaches.
* Regularly update and patch all software components.

## ****6. Mitigation Plan for Top-Priority Threats****

A structured mitigation plan for the top-priority threats is as follows:

|  |  |
| --- | --- |
| Threat | Mitigation Plan |
| Phishing Attacks | Implement anti-phishing tools, conduct security training, enable email filtering. |
| Ransomware Attacks | Implement regular data backups, deploy endpoint security, restrict user permissions. |
| Privilege Escalation | Enforce least privilege access, monitor privileged accounts, implement role-based access control. |
| API Exploitation | Secure API endpoints with authentication tokens, enforce rate limiting, implement API logging. |
| Data Leakage | Apply data loss prevention (DLP) policies, enforce encryption, implement secure logging mechanisms. |

## ****7. Threat Modeling Using IriusRisk****

Threat modeling for the core banking system was conducted using IriusRisk, identifying critical risk areas and recommended controls. The model includes:

* **Assets:** User credentials, financial transactions, customer data.
* **Threat Scenarios:** Unauthorized access, fraud, system tampering.
* **Suggested Mitigations:** Secure coding practices, real-time fraud detection mechanisms, enhanced monitoring.

## ****8. Conclusion****

This security assessment highlights key threats to the core banking system and provides a comprehensive mitigation strategy. By implementing the recommended technical, procedural, and policy-based controls, the organization can significantly reduce security risks and enhance resilience against cyber threats.

## ****9. Recommendations****

* Adopt a proactive security approach with continuous monitoring.
* Conduct regular security assessments and penetration testing.
* Invest in employee security awareness programs.