Cybersecurity Plan for Kentech Banking Project

Overview

This cybersecurity plan provides a structured and platform-agnostic approach to securing the Kentech Banking application, database infrastructure, and network environment. It focuses on data protection, access control, network security, compliance adherence, incident response, and ongoing monitoring applicable to any deployment platform.

Data Protection

- **Encryption:**
  - Data at Rest: Employ robust encryption standards such as AES-256.
  - Data in Transit: Utilize TLS/SSL encryption universally for data transmissions.
- **Database Security:**
  - Enforce strict data validation and constraints as defined in the data dictionary (e.g., account types, card statuses, loan statuses).
  - Implement robust database access control mechanisms using role-based access and granular permissions.

2. Access Control

- **Identity and Access Management (IAM):**
  - Adopt a comprehensive IAM strategy based on the principle of least privilege.
  - Regularly audit roles and permissions to maintain optimal security.
- **Multi-Factor Authentication (MFA):**

    - Require MFA for administrative and sensitive user operations.
- **Role-Based Access Control (RBAC):**
    - Integrate RBAC throughout the application for efficient management of user roles and permissions.

3. Network Security

- **Network Architecture:**
    - Design and implement a segmented network architecture with clearly defined public and private zones.
    - Utilize firewall rules and network ACLs to strictly control inbound and outbound traffic based on service-specific requirements.
- **Web Application Firewall (WAF):**
    - Deploy platform-agnostic WAF solutions to protect against common web vulnerabilities (OWASP top 10).
- **Load Balancing and Traffic Management:**
    - Implement secure load balancing and traffic management tools to distribute incoming traffic effectively and securely.

4. Compliance and Auditing

- **Standards Adherence:**
    - Maintain adherence to industry standards such as PCI DSS, SOC 2, and relevant regulatory requirements through continuous auditing and monitoring.
- **Automated Compliance Tools:**
    - Utilize automated compliance and security tools to continuously monitor, detect, and remediate compliance violations and misconfigurations.
    - Integrate continuous security scanning tools (e.g., OWASP ZAP, AWS Inspector) into the CI/CD pipeline to detect vulnerabilities during development.
- **Audit Logging:**

- Maintain comprehensive audit logs to document critical actions and events, accessible for timely review and incident investigation.

5. Incident Response

- **Incident Response Plan:**
  - Develop and document a thorough incident response strategy detailing roles, responsibilities, communication channels, and escalation procedures.
  - Regularly conduct incident response drills and tabletop exercises.
  - Conduct quarterly disaster recovery drills to validate backup restoration and failover processes, documenting RTO (e.g., 4 hours) and RPO (e.g., 15 minutes).
- **Monitoring and Alerting:**
  - Implement continuous monitoring and real-time alerting systems to detect anomalies and suspicious activities proactively.

6. Continuous Monitoring and Improvement

- **Vulnerability Assessments and Penetration Testing:**
  - Schedule regular and systematic vulnerability assessments and penetration tests.
  - Quickly address and remediate identified vulnerabilities.
- **Security Training:**
  - Regularly provide security awareness training to maintain staff vigilance and knowledge of current threats and best practices.
- **Regular Reviews:**
  - Conduct regular security reviews, incorporating feedback, evolving threats, and incident outcomes into continuous improvement initiatives.

7. Risk Management

- **Risk Identification and Mitigation:**

    - Routinely review and update the project's risk register, identifying and addressing high-impact risks like compliance breaches, cost overruns, and performance issues.
- **Platform Independence:**
    - Document and implement flexible architecture principles and clearly defined migration strategies to mitigate platform dependency risks.