To address the lack of adequate network segmentation in Target's payment system, implement a multi-layered architecture that includes strict segmentation of the cardholder data environment (CDE) from other networks using VLANs and firewalls. Additionally, consider architectural patterns such as Zero Trust Architecture and micro-segmentation to enhance security. Here are some detailed solutions and architectural patterns to consider:

1. Network Segmentation

- **Implement VLANs**: Create separate Virtual Local Area Networks (VLANs) for different departments and functions, ensuring that sensitive payment systems are isolated from other parts of the network.
- **Use Firewalls**: Deploy firewalls between VLANs to control traffic and enforce security policies, allowing only necessary communication between segments.
- **Access Control Lists (ACLs)**: Utilize ACLs to restrict access to sensitive data and systems based on user roles and responsibilities.

2. Zero Trust Architecture

- **Assume Breach**: Design the network with the assumption that breaches can occur, requiring verification for every access request regardless of the source.
- **Micro-Segmentation**: Break down the network into smaller segments, applying security controls at each segment to limit lateral movement of attackers.
- **Continuous Monitoring**: Implement real-time monitoring and logging of all network traffic to detect and respond to suspicious activities promptly.

3. Strong Authentication Mechanisms

- **Multi-Factor Authentication (MFA)**: Require MFA for all access to sensitive systems, especially for third-party vendors and remote access.
- **Role-Based Access Control (RBAC)**: Implement RBAC to ensure users have the minimum necessary access to perform their job functions.

4. Third-Party Risk Management

- **Vendor Access Controls**: Establish strict controls and monitoring for third-party access to the network, ensuring that vendors only have access to the resources they need.
- **Regular Security Assessments**: Conduct regular security assessments and audits of third-party vendors to ensure compliance with security policies.

5. Architectural Patterns

- **Service-Oriented Architecture (SOA)**: Use SOA to create loosely coupled services that can communicate securely, allowing for better control over data access and flow.
- **Event-Driven Architecture**: Implement an event-driven architecture to facilitate real-time data processing and monitoring, enhancing the ability to respond to security incidents.

6. Incident Response Plan

- **Develop a Comprehensive Plan**: Create and regularly update an incident response plan that outlines procedures for detecting, responding to, and recovering from security incidents.
- **Regular Training and Drills**: Conduct regular training sessions and drills for staff to ensure they are prepared to respond effectively to security breaches.

By implementing these solutions and architectural patterns, Target can significantly enhance the security of its payment systems and mitigate the risks associated with network segmentation flaws.