Payment Card Industry Data Security Standard (PCI DSS) Compliance Update 4.0

ARTICLE 07.17.23 GUI COZZI

According to the Verizon 2022 Data Breach and Investigations Report, 84% of data breaches entail payment account data, while 93% are driven by financial motives.

Credit card data is highly valuable and sought after by malicious actors, leading to the need for strong security measures. In response to evolving tactics, the Payment Card Industry Data Security Standard (PCI DSS) has introduced version 4.0 to enhance the protection of credit card data.

This guide provides an overview of the major changes introduced in PCI DSS 4.0, categorized as operational requirements (for sales and customer relations) and technical requirements (for information technology group). It aims to help organizations understand and implement these updates to safeguard cardholder data effectively.

Getting Started with PCI DSS 4.0

- Document, assign, and ensure understanding of roles and responsibilities associated with each of these requirements.
- Perform and document risk analysis/assessment for new requirements.
- Broaden the concept of “network segmentation” to include a wider range of segmentation controls.

1. Install and Maintain Network Security Controls

Technical responsibilities for this step include the following:

- Replace “firewalls” and “routers” with “network security controls” to accommodate various technologies.
- Review configurations of network security controls at least once every six months.
- Secure configuration files to maintain the integrity of security controls.
- Implement security controls on any computing device connecting to untrusted networks and the cardholder data environment (CDE).

2. Protect Stored Account Data

Technical responsibilities for this step include the following:

- Minimize data storage through data retention and disposal policies, verified at least every three months.
- Encrypt electronically stored sensitive authentication data (SAD) before authorization.
- Prevent copying or relocation of primary account numbers (PAN) during remote access.
- Use cryptographic hashes or disk/partition-level encryption to render PAN unreadable on removable electronic media.

Operational responsibilities for this step include the following:

- Ensure third parties storing data on behalf of the organization comply with data retention and disposal policies.
- Maintain an inventory of trusted keys and certificates used for PAN transmission over open, public networks.

3. Protect Cardholder Data During Transmission Over Open Networks

Technical responsibilities for this step include the following:

- Confirm the validity and non-revocation of certificates used to safeguard PAN during transmission.
- Maintain an inventory of trusted keys and certificates used for PAN transmission.

4. Protect Systems and Networks from Malicious Software

Technical responsibilities for this step include the following:

- Define the frequency of periodic evaluations for system components not at risk for malware based on targeted risk analysis.
- Implement processes and mechanisms to detect and protect against phishing attacks.

Operational responsibilities for this step include the following:

- Define the frequency of periodic evaluations for system components not at risk for malware based on targeted risk analysis.
- Implement processes and mechanisms to detect and protect against phishing attacks.

5. Develop and Maintain Secure Systems and Software

Technical responsibilities for this step include the following:

- Maintain an inventory of internal, external, and third-party software components for vulnerability and patch management.
- Deploy an automated solution for detecting and preventing web-based attacks on public-facing web applications.
- Manage all loaded payment page scripts by authorizing and assuring their integrity through written justifications.

6. Restrict Access to System Components and Cardholder Data

Technical responsibilities for this step include the following:

- Assign application and system accounts and related access privileges based on the least privilege necessary.
- Review access by application and system accounts on a frequency defined in the risk analysis.
- Increase password length to a minimum of 12 characters (or 8 if the system doesn’t support 12 characters).
- Implement Multi-Factor Authentication (MFA) for all access into the CDE.
- Ensure MFA systems are resistant to replay attacks, cannot be bypassed, and use at least two different authentication factors.

Operational responsibilities for this step include the following:

- Review all user accounts and access privileges, including third-party/vendor accounts, at least every six months.

7. Restrict Physical Access to Cardholder Data

Technical responsibilities for this step include the following:

- Define the frequency and types of inspections for point of interaction (POI) devices in the targeted risk analysis.

8. Log and Monitor All Access to System Components and Cardholder Data

Technical responsibilities for this step include the following:

- Use automated mechanisms for performing audit log reviews.
- Define periodic log reviews for system components not covered by automated mechanisms.
- Detect, alert, and address failures of critical security control systems promptly.

Operational responsibilities for this step include the following:

- Define periodic log reviews for system components not covered by automated mechanisms.

9. Test Security of Systems and Networks Regularly

Technical responsibilities for this step include the following:

- Manage all applicable vulnerabilities not ranked as high-risk or critical.
- Perform authenticated scanning for internal vulnerability assessments.
- Deploy change and tamper-detection mechanisms for HTTP headers and payment pages received by consumer browsers.

10. Support Information Security with Organizational Policies and Programs

Technical responsibilities for this step include the following:

- Document and review cryptographic cipher suites, protocols, hardware, and software technologies annually.
- Document and confirm PCI DSS scope and conduct reviews upon significant changes.
- Review and update the security awareness program annually to address new threats.
- Include threats and vulnerabilities in security awareness training that could impact CDE security.
- Define the frequency of training for incident response personnel based on targeted risk analysis.
- Implement incident response procedures for the detection of unexpected storage of PAN.

Operational responsibilities for this step include the following:

- Support flexible PCI DSS requirements with targeted risk analysis.
- Document and confirm PCI DSS scope annually and upon significant changes.
- Include threats and vulnerabilities in security awareness training, including the acceptable use of end-user technologies.
- Define the frequency of training for incident response personnel based on targeted risk analysis.
- Implement incident response procedures for the detection of unexpected storage of PAN.

Implementing the updated PCI DSS 4.0 requirements is crucial for organizations to protect credit card data from unauthorized access. By following the guidelines outlined in this guide, organizations can enhance their network security, minimize data storage, encrypt sensitive information, restrict access, monitor systems, and support information security with effective policies and programs. Adhering to these measures will help mitigate the risk of credit card data falling into the wrong hands and ensure compliance with the latest PCI DSS standards.