PaymentsEd FORUM

What's New with PCI DSS

Highlights to Key Changes

DRF PAYMENTS EDUCATION

Lib de Veyra, JCB International Credit Card Co., Ltd.

Agenda

1. The PCI Data Security Standard – History and Purpose
2. Development vs. Enforcement of the PCI DSS
3. The PCI DSS Lifecycle
4. Breaking Down PCI DSS v3.2 Revisions
5. Deprecated Internet Protocols
6. Secure Sysadmin Access to Cardholder Data
7. New Requirements for Service Providers

Agenda (continued)

1. Business as Usual and Security Accountability
2. Other Revisions
3. Why Changes Were Made
4. How to Provide Feedback to the PCI DSS
5. Additional Helpful Resources
6. Other Areas PCI SSC is Looking at

The PCI Data Security Standard – History and Purpose

- Flagship standard for the PCI Security Standards Council
- Applies to all entities that store, process and transmit cardholder data
- Cardholder data includes the Primary Account Number, other sensitive card data, and sensitive authentication data (e.g. magnetic stripe data, card authentication values)
- First version published in 2006
- The current version (PCI DSS v3.2) was published in April 2016

Development vs. Enforcement of the PCI DSS

- The PCI Security Standard Council is responsible for:
  - Developing and publishing the PCI DSS through industry stakeholder engagement
  - Administering the assessor programs supporting PCI DSS (Qualified Security Assessors, Approved Scanning Vendors and PCI Forensic Investigators)

- Enforcement of compliance with the PCI DSS is the responsibility of the payment card brands.

The PCI DSS Lifecycle

- Historically, the PCI DSS undergoes a revision every two to three years
- In between those cycles, minor revisions have been published usually to address clarifications and make minor corrections
- The PCI Council reserves the right to publish new revisions mid-cycle to address emerging threats and vulnerabilities more swiftly
- For example, PCI DSS v3.1 was published in between cycles to address the deprecation of insecure internet protocols

Breaking Down PCI DSS v3.2 Revisions

- Insecure internet protocols - change in sunset dates and additional requirements
- Business as usual and security accountability incorporated
- Multi-factor authentication for administrator access to the cardholder data environment
- Service providers - new requirements with future effective dates
- Others

Insecure Internet Protocols

- SSL and early TLS are considered insecure internet protocols per security researchers and the National Institute of Standards and Technology (NIST)
- Prior sunset dates in PCI DSS v3.1 were deemed too aggressive so changes were made to extend those dates
- New implementations must use secure protocols
- Service providers must provide secure protocol offering to their customers
- Prior to June 30, 2018, migration plan from insecure to secure protocols
- After June 30, 2018, no use of insecure protocols (exception for point of interaction devices not susceptible to exploits)
- New Appendix A2 covers additional requirements

Secure Sysadmin Access to Cardholder Data Environment

- All system administrators must access the cardholder data environment using multi-factor authentication
- Previously reserved only for all remote access to the cardholder data environment (still a requirement)
- Adds layer of protection due to stolen or maliciously obtained user IDs and passwords by system administrators

New Requirements for Service Providers

- Additional requirements have future effective dates of February 1, 2018
- Maintain documented description of cryptographic architecture
- Detect and alert on critical security control failures
- Penetration testing every six months (instead of just annually)
- Perform quarterly reviews to confirm personnel are following security policies

Business as Usual and Security Accountability

- Change control processes must include verification of PCI DSS requirements impacted by change
- Accountability and responsibility at executive leadership or equivalent and a PCI DSS compliance program

Other Revisions

- Clarified that certain requirements also apply to payment applications
- Provide flexibility in masking due to legitimate business needs (future increase in BIN range lengths and PAN lengths)
- Added the additional requirements for Designated Entities to the Appendix section

Why Changes Were Made

- Exploits found in data breach investigations
- New threats and vulnerabilities identified in the security intelligence community
- Impact of emerging technologies
- Legal and regulatory considerations
- Provide flexibility to requirements
- Provide additional guidance on intent of requirements

How to Provide Feedback on the PCI DSS

- Join as a Participating Organization at the PCI Security Standards Council
- Participate in Special Interest Groups and Task Forces on different security subjects
- Nominate your company to be on the Board of Advisors
- Provide feedback through association memberships
- Submit questions through the PCI SSC website

Additional Helpful Resources

- White paper on scoping and segmentation to be published later this year
- Variety of documents targeted at small merchants
- Existing information supplements on specific subjects
  - Telephone-Based Payments
  - Penetration Testing
  - Risk Assessment
  - Third Party Security Assurance
  - Phishing
  - Virtualization
- PCI Website: pcisecuritystandards.org

Other Areas PCI SSC is Looking at

- Mobile payment applications
- Mobile PIN entry
- Mobile payment provisioning (HCE and SE)
- Mobile in-app purchases
- Internet of things
- A simpler approach to PCI DSS particularly for small merchants

JCB International Credit Card Co., Ltd.

Contact me at:

lib.deveyra@jcbusa.com

Lib de Veyra

Vice President, Emerging Technologies

If you have any questions about the presentation, go to our LinkedIn Group (the Payments Education Forum) and request an invitation (this is a closed group specifically for the payments industry).