Thater & Schwier
Consulting

Payment Card Industry Data Security Standard (PCI DSS)

Frank Thater

3-May-2016

frank.thater@tscons.de

https://www.tscons.de

Agenda

- Motivation and Payment Card Industry (PCI) History
- PCI DSS Requirements
- PCI DSS Assessment Process
- PCI DSS vs. ISO 27001

Motivation

- Payment card fraud (some examples)
  - 90.000.000 account data sets stolen from U.S. retailer
  - Ticket provider „lost“ 60.000 account data sets
  - 45 mio US-$ stolen by single hacker group with account data stolen from payment processing system
- Lucrative business for criminals
  - Up to 90 Dollar per stolen account data set
- Protection of account data
- Protection of credit institutions risk

Payment Card Industry History

- Founded in 2001
  - Visa Cardholder Information Security Program
  - MasterCard
- Developed by Visa und MasterCard
- Set of common security requirements derived from specific requirements of payment brands
- Version 1.0 released in 2004
- PCI Security Standards Council founded in 2006
  - MasterCard, Visa, JCB, American Express, Discover

PCI Security Standard Council (SSC)

- Responsible for all PCI Standards
  - Data Security Standard (PCI DSS)
    - Merchants and Service Providers
  - Payment Application Data Security Standard (PCI PA DSS)
    - Development of payment applications
  - PIN Transaction Security (PCI PTS)
    - Payment terminal vendors
  - Hardware Security Module
- Qualifies companies for assessment process
  - (PA-) Qualified Security Assessors (QSA)
  - PCI Forensic Investigators (PFI)
  - Approved Scanning Vendor (ASV)

What should be protected?

- Account Data
  - Cardholder Data
    - Primary Account Number
    - Cardholder Name
    - Expiration Code
    - Service Code
  - Sensitive Authentication Data
    - Full track data
    - CAV2/CVC2/CVV2/CID
    - PIN

PCI Data Security Standard (DSS)

- Set of requirements to protect account data in the complete (cardholder data) processing environment, including
  - POS-Terminals and merchant environment
  - (Payment) Service Provider
  - Acquirer
  - Issuer
- 12 security requirements and 310 testing procedures to protect account data (Version 3.1, 2015)
- Annually assessment mandated by payment brands
  - Form and scale of the assessment vary significantly depending on the size of the merchant or service provider

PCI DSS Requirements 1 - 6

- Build and Maintain a Secure Network and Systems
  - Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data
  - Requirement 2: Do Not Use Vendor-supplied Defaults for System Passwords and Other Security Parameters
- Protect Cardholder Data
  - Requirement 3: Protect Stored Cardholder Data
  - Requirement 4: Encrypt Transmission of Cardholder Data Across Open Public Networks
- Maintain a Vulnerability Management Program
  - Requirement 5: Use and Regularly Update Antivirus Software or Programs
  - Requirement 6: Develop and Maintain Secure Systems and Applications

PCI DSS Requirements 7 - 12

- Implement Strong Access Control Measures
  - Requirement 7: Restrict Access to Cardholder Data by Business Need-to-know
  - Requirement 8: Assign a Unique ID to Each Person with Computer Access
  - Requirement 9: Restrict Physical Access to Cardholder Data
- Regularly Monitor and Test Networks
  - Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data
  - Requirement 11: Regularly Test Security Systems and Processes
- Maintain an Information Security Policy
  - Requirement 12: Maintain a Policy That Addresses Information Security for All Personnel

Example - PCI DSS Requirement 3.2.2

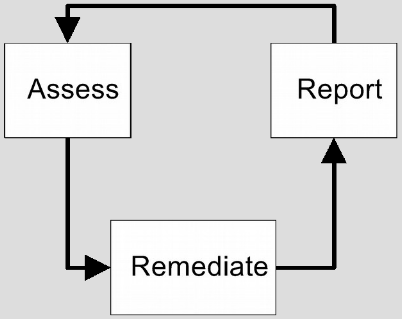
- Protect Stored Cardholder Data
- Requirement
  - „3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization."
- Testing Procedure
  - „3.2.2 For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization:
    - Incoming transaction data
    - All logs (for example, transaction, history, debugging, error)
    - History files
    - Trace files
    - Several database schemas
    - Database contents."

Example - PCI DSS Requirement 7.3

- Restrict access to cardholder data by business need to know
- Requirement
  - „7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.“
- Testing Procedure
  - „7.3 Examine documentation and interview personnel to verify that security policies and operational procedures for restricting access to cardholder data are:
    - Documented,
    - In use, and
    - Known to all affected parties.“

PCI DSS Assessment Process

- **Assess**
  - Identify cardholder data flow in business processes
  - Assess gaps and identify risks
- **Remediate**
  - Implement remediation plan
- **Report**
  - On-Site Assessment
  - Self-Assessment Questionnaire (SAQ)
  - ASV scan report
  - Report on Compliance (ROC)
  - Report to acquirer and payment brand



PCI DSS vs. ISO 27001 - I

- Some PCI DSS requirements are related/can be mapped
  - DSS Requirement 4: Encrypt Transmission of Cardholder Data Across Open Public Networks
    - A.10 Cryptography
    - A.13 Communications security
  - DSS Requirement 6: Develop and Maintain Secure Systems and Applications
    - A.14 System acquisition, development and maintenance
  - DSS Requirement 7: Restrict Access to Cardholder Data by Business Need-to-know
    - A.9 Access control
  - DSS Requirement 9: Restrict Physical Access to Cardholder Data
    - A.11 Physical and environmental security
  - DSS Requirement 12: Maintain a Policy That Addresses Information Security for All Personnel
    - A.5 Information Security policies
    - A.6 Organization of information security
    - A.7 Human resource security
    - A.8 Asset management
  - DSS Requirements 1, 5, 10, 11
    - A.12 Operations security

PCI DSS vs. ISO 27001 - II

- PCI DSS Continous Improvement Process
  - But not a complete ISO 27001 ISMS
- Best practice security controls
  - ISO 27002 as an additional source for practices
- Different certification schemes
  - „Global value“ ISO certification vs. „Specific“ SSC and Payment Brand assessment
- PCI DSS can be integrated in an ISMS
  - A.18 Compliance

Questions?

Comments?

frank.thater@tscons.de

Backup - Payment Brand Conformity Assessment

- Depends on payment brand
  - American Express
    - www.americanexpress.com/datasecurity
  - Discover
    - www.discovernetwork.com/fraudsecurity/disc.html
  - JCB International
    - www.jcb-global.com/english/pci/index.html
  - MasterCard Worldwide
    - www.mastercard.com/sdp
  - VISA
    - Visa Inc - www.visa.com/cisp
    - Visa Europe - www.visaeurope.com/ais

Backup - Merchant Classification

	MasterCard	Visa / Discover	Amex	JCB
Level 1	> 6 mio transactions per year 1 security incident in the past	> 6 mio transactions per year 1 security incident in the past	> 2,5 mio transactions per year 1 security incident in the past	> 1 Mio transactions per year 1 security incident in the past
Level 2	1 - 6 Mio mio transactions per year (MasterCard + Maestro)	1 - 6 mio transactions per year	50.000 - 2,5 mio transactions per year	< 1 Mio transactions per year
Level 3	20.000 - 999.999 transactions per year (MasterCard + Maestro)	20.000 - 1 mio transactions per year	< 50.000 transactions per year	n/a
Level 4	< 20.000 transactions per year	< 20.000 transactions per year	n/a	n/a

Backup - Impact of Classification

- Depending on the level the merchant must perform different assessment tasks
- Sample
  - Level 1, MasterCard
    - ASV scan, QSA on-site assessment
  - Level 2, Visa
    - ASV scan, SAQ self-assessment
  - Level 4, MasterCard
    - ASV scan (if requested from the acquiring bank), SAQ self-assessment