Protect your business with PCI DSS

Raden Ardiansyah Natakusumah

July 27th, 2017

About Me

- https://about.me/r_u_l_l_y

Introduction

- Payment Card Industry Data Security Standard
  - provides a baseline of technical and operational requirements designed to protect account data
  - applies to all entities involved in payment card processing (merchants, processors, acquirers, issuers, and service providers)
  - applies to all other entities that accept, store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD)
  - 6 primary goals, 12 requirements, more than 400 sub requirements

Overview

Six Goals, Twelve Requirements

Six Goals	12 Requirements
Build and Maintain a Secure Network and Systems	• Install and maintain a firewall configuration to protect cardholder data • Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	• Protect stored cardholder data • Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	• Protect all systems against malware and regularly update anti-virus software or programs • Develop and maintain secure systems and applications
Implement Strong Access Control Measures	• Restrict access to cardholder data by business need-to-know • Identify and authenticate access to system components • Restrict physical access to cardholder data
Regularly Monitor and Test Networks	• Track and monitor all access to network resources and cardholder data • Regularly test security systems and processes
Maintain an Information Security Policy	• Maintain a policy that addresses information security for all personnel

Where? Who?

- Sensitive data (PII, cardholder data)
  - where's the location?
  - who responsibility for it?

- If You Don't Need It, Don't Store It!
  - need to be retained and stored?
  - more items you can remove, the better

Defense in depth

- Perimeter (WAF) firewall
- IPS
- File Integrity Monitoring
- Limiting remote access
  - Use multi factor authentication
- Anti virus
- Patch
- Regular vulnerability assessment and penetration testing

People

- Regular security awareness

How to comply?

- Scoping
  - determine which system components and networks are in scope
- Assessing
  - examine the compliance of system components in scope following the testing procedures for each requirement
- Reporting
  - assessor and/or entity submits required documentation (SAQ, RoC, compensating controls)
- Clarification
  - assessor and/or entity clarifies/updates report statements (if applicable) upon request of the acquiring bank or payment card brand

Scoping

- How many applications store, process or transmit cardholder data?
- How many databases support the in-scope applications?
- List all database platforms that store credit card data (Oracle, MS SQL, DB2)?
- How many servers store, process or transmit cardholder data to support the applications in scope?
- What are the operating systems for the servers (MS, UNIX, Linux, AS400, etc.)?
- Is there segmentation between the systems storing credit card data and the rest of the network?
- How many Internet, DMZ, or segmentation firewalls are in place?
- How is the segmentation achieved (VLAN, Firewall, etc.)?
- Is wireless technology in use anywhere on the network? If so, how many locations?
- Is credit card data transmitted over wireless devices at any point?
- Are credit card transactions accepted through a web server?
- Are credit card numbers stored on the POS systems for any length of time?
- How many data centers store, process or transmit cardholder data?
- How many call centers store, process or transmit cardholder data?
- Is any part of the environment outsourced?
- Are there third parties, outsourcers, or business partners connected to the network?

Requirement 1

- Install and maintain a firewall configuration to protect cardholder data

- Requirement 1.4
  - Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE.

Requirement 3

- Protect stored cardholder data

- If you don’t need it, don’t store it!

Requirement 4

- Requirement 4.2

- Never send unprotected PANs by enduser messaging technologies (for example, email, instant messaging, SMS, chat, etc.).

Requirement 5

- Protect all systems against malware and regularly update anti-virus software or programs
  - Malicious software, commonly reffered to as “malware” – including viruses, worms, and Trojans- enters the network during many business-approved activities including employee email and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities
  - Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats
  - Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place

Requirement 6

- Develop and maintain secure systems and applications
  - Secure authentication and logging
  - Based on industry standards/ best practices
  - Secure SDLC
  - Remove development and test accounts and data before deploy to production
  - Perform security code review

Requirement 6 (Contd.)

- Separate development, test, and production environments
- Don’t use production data for testing or development
- Change control processes and procedures for all changes
- Upon completion of significat change, all relevant PCI DSS requirements must be implemented
- Secure coding techniques training, at least annually
- Conduct application vulnerability assessments

Requirement 8

- Revoke access for terminated users
- Remove/ disable inactive user accounts
- Accounts are locked after 6 invalid logon
- Session idle no more than 15 minutes
- Password policy
  - Minimum 8 characters alphabetic and numeric characters
  - Changed at least every 90 days
  - Don’t use the same previous 4 passwords

Requirement 9

- Restrict physical access to cardholder data
  - Physical controls (e.g. Badge readers, authorized badges, lock & key)
  - Video cameras/ CCTV and access control mechanisms
  - Network jacks must be proctected or disabled in public areas
  - Restrict physical access to wireless access points, gateways, networking and communication hardwares, etc

Requirement 9 (Contd.)

- Assign badges for personnel or visitors
  - Visibly distinguishes the visitors from onsite personnel
- Revoking or terminating expired ID badges
- Access is revoked immediately upon termination, and any keys, access cards, etc., returned or disabled
- Maintain a visitor log
- Destroy media when it is not needed for business or legal reasons
  - Shred, incinerate, or pulp hard-copy materials
  - Secure delete/wipe program

Requirement 9 (Contd.)

- Card-reading devices used in card-present transactions (swipe or dip) at the point of sale
- List of devices – make, model, location, unique identifier (e.g. Serial number)
- Periodically inspect device surfaces to detect tampering or substitution
- Training for personnel
  - Follow procedures for handling devices, aware for suspicious behavior, reported

Requirement 12

Requirement 12: Maintain a Policy That Addresses Information Security for All Personnel

- A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it
- For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment

Benefits

- Peace of mind
  - you won't have to worry quite as much about any potential vulnerabilities in your system
- Increasing consumer trust
  - more business = increase revenue
- Protecting image and reputation
  - Account Data Compromise (breach), requires a Merchant to communicate an incident to their customers

Breaches = Fines!

- Up to US$ 20,000, inspection fees from independent PCI Forensic Investigator
- Non-compliant:
  - Up to US$ 500,000, data security fine
  - Up to US$ 50,000/ day, non-compliance fines
  - Up to US$ 10/ card X total numbers of cards compromised
- Refund fees, for all fraud losses incurred from compromised account

Conclusion

- Focus on security, not compliance

Questions?


blibli.com
BIG CHOICES BIG DEALS


THANK
YOU