New Paltz
STATE UNIVERSITY OF NEW YORK

PCI Compliance

The experience at New Paltz
a.k.a. “The Good, the Bad,
and the Ugly”

SUNY Technology Conference
Lake Placid - June 2015
Paul Chauvet

Why are we here?

Why are we here?

Why are we here?

Why are we here?

- Data breaches
- Compliance
- Acquirer/processor pressures

Who I am

- Paul Chauvet (chauvetp@newpaltz.edu)
- Information Security Officer at New Paltz since 2014
- Systems Admin at New Paltz 2003-2014

What I am not

- I am not a QSA
- I am not a lawyer
- I don’t know your environment
- I can’t tell you for certain which SAQ you should complete.

Terms

- Scope
- ASV - Approved Scanning Vendor
- QSA - Qualified Security Assessor
- PCI-DSS - Payment Card Industry Data Security Standard
- PA-DSS - Payment Application Data Security Standard
- SAQ - Security Assessment Questionnaire

Terms

- Cardholder Data
  - Primary Account Number
  - Cardholder name
  - Expiration date
  - Service Code
- Sensitive Authentication Data
  - Full track data
  - CVV
  - PIN

What is the Scope of PCI?

applies to "*all **system components** in **<u>or connected to</u>** the cardholder data environment*"

Examples of scope:

- Virtualization environment
- Network equipment (switches, access points, routers)
- Systems involved in or providing services to cardholder data environment (DNS, NTP, authentication, proxy, web)
- Any system or component connected to the CDE

Scope - Why do we care?

Cardholder data is a virus

Limit the spread as if it were an infectious disease.

How can scope be reduced?

- Network Segmentation
- Point-to-Point Encryption (P2PE)

To be considered out of scope for PCI-DSS, a system component must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised, it could not impact the security of the CDE.

ARMY
Aéropostal

New Paltz
STATE UNIVERSITY OF NEW YORK

Things to avoid if possible

- Electronic storage of credit card data in ANY format (even encrypted)
- Taking credit cards over the phone via VoIP

What if you find out you are storing card data electronically...

How can scope be reduced?

- Network Segmentation
- Point-to-Point Encryption (P2PE)
  - Encrypted at swipe
  - You should be completely unable to see/access unencrypted card data.

To be considered out of scope for PCI-DSS, a system component must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised, it could not impact the security of the CDE.

Network restrictions

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network.

System Hardening

- Center for Internet Security - Benchmark Tools
- Dedicated Payment Systems
  - Don’t use wireless keyboards
- Two factor authentication for system components.
- File integrity monitoring

Patch Management

- Need a local patch repository
- *“Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations.”*

Software Development

- Consider using outside vendors for all credit card processing software.
- Avoid using in-house code development for anything involving credit card processing. Doing so requires:
    - Code review by knowledgeable individuals *other than* the code authors
    - Lots of change controls and change documentation
    - Secure coding techniques training needed

Vulnerability Management

- Internal vulnerabilities on all *system components*.
  - Performed by a *qualified internal resource*
- External scanning and remediation on all public facing systems in your network
  - Performed by an *Approved Scanning Vendor (ASV)*

Penetration Testing

- External testing must be done at least annually or after significant changes.
- Must be done by a qualified internal resource that is **organizationally independent** or a qualified external tester.
- Network segmentation must be verified/tested.

Physical Requirements

- Much more stringent requirements when cardholder data is stored.
  - Even more if removable media is used for storage
- Inspection of hardware is a necessity
- Destroy hard copies when done processing

Monitoring

10.6.1 - Review the following at least daily ***(either manually or via log tools)****:*

- *All security events*
- *Logs of all system components that store, process, or transmit CHD and/or SAD*
- *Logs of all critical system components.*
- *Logs of all servers and systems that perform security functions (for example, firewalls, IDS/IPS, authentication servers, e-commerce redirection servers, etc.)*

10.7 - Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis

Policy Review

- Review your Information Security Policies
- Fill in any identified policy gaps
- Make sure the CC processing staff understand the policy
- Background checks
- Have an incident response policy
    - Test your incident response plan

Challenges

- External agencies on your network (bookstore, food services, auxiliary services)
- Getting your acquirer to accept compensating controls or acceptable risks
- Wireless Access Points

Wireless Access Points

11.1 - Implement processes to test for the presence of wireless access points, and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

On a college campus?

Seriously?

No.

Not happening.

No way.

Questions? Comments?