ACI UNIVERSAL PAYMENTS

PCI DSS 3.2 CHANGES

Planning for the Next PCI Assessment

January 20, 2017

Lisa McKee, PCIP

Agenda

- *New Requirements effective now*
- *New Requirements effective January 31, 2018*
- *Updated Requirements*
- *SSL/Early TLS*
- *Next Steps*

PCI DSS 8.3.2

- Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.

Agenda

New Requirements effective now

New Requirements effective January 31, 2018

Updated Requirements

SSL/Early TLS

Next Steps

PCI DSS 3.5.1

- ***Additional requirement for service providers only:*** Maintain a documented description of the cryptographic architecture that includes:
- Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date
- Description of the key usage for each key.
- Inventory of any HSMs and other SCDs used for key management

Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

PCI DSS 6.4.6

- Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

PCI DSS 8.3.1

- Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.

Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

PCI DSS 10.8

- ***Additional requirement for service providers only***: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:
  - Firewalls
  - IDS/IPS
  - FIM
  - Anti-virus
  - Physical access controls
  - Logical access controls
  - Audit logging mechanisms
  - Segmentation controls (if used)

Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

PCI DSS 10.8.1

- ***Additional requirement for service providers only***: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:
  - Restoring security functions
  - Identifying and documenting the duration (date and time start to end) of the security failure
  - Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause
  - Identifying and addressing any security issues that arose during the failure
  - Performing a risk assessment to determine whether further actions are required as a result of the security failure
  - Implementing controls to prevent cause of failure from reoccurring
  - Resuming monitoring of security controls

  Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

PCI DSS 11.3.4.1

- ***Additional requirement for service providers only:*** If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.

Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

PCI DSS 12.4.1

- ***Additional requirement for service providers only:*** Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:
  - Overall accountability for maintaining PCI DSS compliance
  - Defining a charter for a PCI DSS compliance program and communication to executive management

Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

PCI DSS 12.11

- ***Additional requirement for service providers only:*** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:
  - Daily log reviews
  - Firewall rule-set reviews
  - Applying configuration standards to new systems
  - Responding to security alerts
  - Change management processes

Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

PCI DSS 12.11.1

- ***Additional requirement for service providers only:*** Maintain documentation of quarterly review process to include:
  - Documenting results of the reviews
  - Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program

Note: *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*

Agenda

New Requirements effective now

New Requirements effective January 31, 2018

- *Updated Requirements*

SSL/Early TLS

Next Steps

PCI DSS 1.1.6.a

- Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and **approval for each**.

PCI DSS 2.1

- Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, **payment applications**, Simple Network Management Protocol (SNMP) community strings, etc.

PCI DSS 6.4.5.a

- Examine documented change-control procedures and verify procedures are defined for:
  - Documentation of impact.
  - Documented change approval by authorized parties.
  - Functionality testing to verify that the change does not adversely impact the security of the system.
  - Back-out procedures.

  – **v3.1 explicit to patches and software modifications, v3.2 applies to all changes of any kind**

PCI DSS 6.5

- Address common coding vulnerabilities in software-development processes as follows:
  - Train developers **at least annually** in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.
  - Develop applications based on secure coding guidelines.

PCI DSS 8.5.1

- Manage IDs used by **third parties** to access, support, or maintain system components via remote access as follows:
  - Enabled only during the time period needed and disabled when not in use.
  - Monitored when in use.

PCI DSS 12.8.1

- Maintain a list of service providers **including a description of the service provided**.

Agenda

New Requirements effective now

New Requirements effective January 31, 2018

Updated Requirements

- *SSL/Early TLS*

Next Steps

PCI DSS Appendix A2

PCI Security Standards Council

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

Entities using SSL and early TLS must work towards upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits.

The PCI DSS requirements directly affected are:

Requirement 2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
Requirement 2.3	Encrypt all non-console administrative access using strong cryptography.
Requirement 4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

SSL and early TLS should not be used as a security control to meet these requirements. To support entities working to migrate away from SSL/early TLS, the following provisions are included:

- New implementations must not use SSL or early TLS as a security control
- All service providers must provide a secure service offering by June 30, **2016**
- After June 30, **2018**, all entities must have stopped use of SSL/early TLS as a security control, and use only secure versions of the protocol (an allowance for certain POS POI terminals is described in the last bullet).
- Prior to June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.
- POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS, may continue using these as a security control after 30th June, 2018.

This Appendix applies to entities using SSL/early TLS as a security control to protect the CDE and/or CHD (for example, SSL/early TLS used to meet PCI DSS Requirement 2.2.3, 2.3, or 4.1), Refer to the current *PCI SSC Information Supplement Migrating from SSL and Early TLS* for further guidance on the use of SSL/early TLS.

PCI DSS 2.2.3

- Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.

Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.

PCI DSS 2.3

- Encrypt all non-console administrative access using strong cryptography.

Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.

PCI DSS 4.1

- Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:
  - Only trusted keys and certificates are accepted.
  - The protocol in use only supports secure versions or configurations.
  - The encryption strength is appropriate for the encryption methodology in use.

Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.

PCI DSS A2.1

- Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either:
  - Confirm the devices are not susceptible to any known exploits for those protocols.

  Or:

  - Have a formal Risk Mitigation and Migration Plan in place.

PCI DSS A2.2

- Entities with existing implementations (other than as allowed in A.2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.

PCI DSS A2.3

- ***Additional Requirement for Service Providers Only:*** All service providers must provide a secure service offering by June 30, 2016.

Note: *Prior to June 30, 2016, the service provider must either have a secure protocol option included in their service offering,* ***or*** *have a documented Risk Mitigation and Migration Plan (per A.2.2) that includes a target date for provision of a secure protocol option no later than June 30, 2016. After this date, all service providers must offer a secure protocol option for their service.*

Agenda

New Requirements effective now

New Requirements effective January 31, 2018

Updated Requirements

SSL/Early TLS

Next Steps

Next Steps

- ***Start talking and planning for this now***
  - Takes time to make changes
  - New Requirements (10)
  - Updated Requirements (6)
  - SSL/Early TLS (6)
- ***Set target completion dates***
  - Example: Requirement effective January 31, 2018 set date as September 30, 2017
- ***Work with your QSA***
  - Understand their expectations