PCI DSS 3.2

Evolution of Point of Sale and Online Payment Safeguards

Author:

Hariharan Anantha Krishnan,

Principal Consultant & Practice Manager,

Consulting Services

PALADION

HIGH SPEED CYBER DEFENSE

PCI Security Standard Council's latest update to the PCI DSS standard guarantees cardholder data protection on recovery sites, masking standards for card numbers, multifactor verification for personnel, and more. This paper outlines the upgrades from PCI 3.1 to PCI 3.2. If you have not yet implemented the 3.1 standard, please take a look at our step by step guide to transition from 3.0 to 3.1.

The council has given sufficient time for merchants to incorporate these changes; most upgrades will be effective from February 2018.

The Need for PCI DSS

There is no doubt that the threats associated with online payments have substantially increased, which is exactly why there has always been a pressing need to stay ahead of the curve when it comes to online payment safeguards. The PCI Security Standards Council launched an updated version of the Payment Card Industry Data Security Standard with PCI DSS 3.2, earlier this year in April.

The newer version is a testament to the fact that it provides merchants, businesses, and consumers with powerful features and benefits, so that they can always remain safe against the ever evolving and changing online threats.

A Newer and More Powerful Update

The purpose of the update by the Council is to make sure that PCI DSS consistently and efficiently continues to reduce, and potentially eliminate the chances of any sort of complications that are still an issue. Plus, the new update is also for providing new exploits, giving users a more precise picture of how they can efficiently incorporate the implementation of the PCI DSS interface. It is important to realize that version 3.1 is going expire at the end of October 2016.

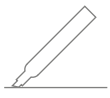
Version 3.2 and Why It is Preferred Over the Standard 4.0

PCI DSS has become a reliable standard in the industry today. Businesses and organizations consider it to be an effective and efficient standard. PCI DSS 3.2 does not require constant updates, which has been the case with earlier and existing versions. Furthermore, vendors and the overall markets can expect the newer and improved version to completely revamp the traditional threat and payment environment with precise emphasis on providing merchants and payment vendors with increased clarity and a step by step walkthrough to enable companies to utilize version 3.2 as a traditional and daily business standard and practice.

PCI DSS 3.2 - What's New?

The primary factor that has driven the need to revise standard features are more importantly based on the basis of the continual and changing nature of the threats to online transactions, the relevant feedback gathered through community meetings in the market, and the urgency of making all the necessary clarifications.

In all, version 3.2 is a powerful improvement over the previous version and is significantly better when you talk about clarifications and integrating or employing newer technologies into your business. However, it is important to realize the fact that there has been no drastic change implemented in the core 12 requirement of the standard software. However, businesses and organizations can be rest assured regarding the increased transparency and consistency of version 3.2.



The Key Highlights & Changes Made

Clarification of the need of recovery must be considered

In version 3.2, the standard clearly states that the backup as well as the recovery data of the websites will have to be thoroughly reviewed and assessed by the QSA in order to safely quantify its scope in terms of control applicability. In simpler terms, the version guarantees cardholder data protection on recovery sites.

Clarification of the display of credit card number exceeding the first six or the last four digits

A majority of business organizations implement a plethora of masking standards in specific instances - making it essential to view the 7th and 8th digit of any credit card. However, in version 3.2 it has been made clear that the users are not allowed to view credit card digits that exceed the first 6or the last 4digits without a legitimate business justification.

The necessity of keeping documented description of cryptographic architecture

(Effective from February 1, 2018)
This change was mostly integrated for service providers in order to sustain recorded details of cryptographic architecture, which primarily includes key specifications, algorithms, inventory of HSMs, etc. This change in requirement can be implemented as a best practice till January of 2018 and will be made mandatory the same year.

Change control process to be verified by PCI DSS

(Effective February 1, 2018)
The primary reason for the implementation of this change is to ensure that there is no lapse in any security protocols whenever there is a change or altercation in production. This standard makes it mandatory for businesses to establish a set of processes to authenticate all applicable PCI DSS specifications, and to ascertain that all requirements are incorporated on all new or altered system components.

Multifactor verification for personnel with remote and non-console admin access

(Effective February 1, 2018)
Requirement 8.3 of the new standard has required a multi factor authentication for remote access to systems.

The council has tried to emphasize that organizations should consider two or more factor of authentication against just "two-factor authentication" requirement in PCI DSS v3.1. Moreover, this change has also introduced a new specification, providing secure access to CDE by incorporating multifactor-authentication for all personnel that have non-console access to the CDE.

Quick identification of critical security failures

(Effective February 1, 2018)
This change is solely meant for Service Providers. The main function of the change is to ensure all essential system elements such as firewalls, IPS/IDS, FIM, anti-virus, SIEM, etc. remain secured and are available at all times – providing quick and timely alerts in case of any critical system failure within the CDE.

Established responsibilities to protect cardholder data and to ensure full PCI DSS compliance

(Effective February 1, 2018)
This change too is meant only for Service Providers and ensures visibility to executive-level personnel into PCI DSS compliance components in order to identify the efficiency and effectiveness of the program - highlighting core security opportunities and strategy.

Quarterly reviews to affirm the implementation of all security policies and operational processes

(Effective February 1, 2018)
The new change applies only to Service Providers, giving birth to newer procedures for authenticating critical security elements and processes. This specification makes it important for organizations to make quarterly reviews and to ensure that Business-as-Usual security protocols are being followed at all times.

New appendix - additional requirements for organizations using SSL/Early TLS, implementing new migration deadlines

(Effective February 1, 2018)
An addition to the appendix sheds light on the importance of integrating migration controls for risks attached to SSL/ early TLS. The appendix also provides a reference to documents given by the Council on information supplement migrating from SSL as well as early TSL.

New appendix to integrate designated entities supplemental validation

(Effective February 1, 2018)
This appendix, which was previously a separate document - in the newer version, applied only to organizations designated by a payment brand(s) or an acquirer as needing additional authentication of existing PCI DSS specifications, for example, breached entities. The new supplemental authentication process is a step towards ensuring greater PCI DSS controls and accessibility that are continuously maintained through the validation of Business-as-Usual processes.

A Giant Leap towards the Future of Secured Payment Portals

The only way forward for businesses that are seeking PCI DSS certification or compliance through self-assessment for the first time is to evaluate these changes in the newer version. For business organizations and service providers that already have certification of the previous version - the way forward is to perform an intermediate gap assessment for the new / upgraded requirements in the newer version and implement the required additional controls to efficiently comply with all additional changes.

PALADION
HIGH SPEED CYBER DEFENSE

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668.
Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net