How to Secure the Cardholder Data Environment and Achieve PCI Compliance?

VISTA INFOSEC®
TRUSTED ADVISORS ASSURED COMPLIANCE

Any business dealing with the Cardholder Data, the security of that data, and the Cardholder Data Environment should be the top-most priority. This is not just from the PCI DSS Compliance perspective, but, also from the security perspective against incidents of Data Breach or Data Theft. Businesses should ensure that the Cardholder Data Environment in which the sensitive data is processed, stored, or transmitted is completely secure. Although this could be a very stressful and expensive process, yet ensuring data protection and security implementation around the Cardholder Data Environment is mandatory and not really an option. Covering more on this in detail, we have written a detailed article that will help Merchants and Service Providers in securing the Cardholder Data Environment and achieving PCI Compliance. But, let us first understand the meaning of the Cardholder Data Environment before learning how it can be secured.

What is Cardholder Data Environment?

The Cardholder Data Environment comprises systems that store and process card data, and networks that transmit card data. This could even include third-party service providers, vendors, or entities who handle or have access to cardholder data in the organization. Including people and processes that are directly or indirectly a part of card data processing. Basically, any system, network, or technology that holds card data and the sensitive authentication data becomes a part of your Card Data Environment.

PCI DSS Requirements for Securing Cardholder Data Environment

The Payment Card Industry Data Security Standard outlines specific requirements to secure the digital payment and authentication of cardholder data in rest or transit. This means securing card data and authentication data in any system, physical devices, network, or virtual components in the Card Data Environment. The requirements include-

- Install and maintain networking security like the firewall and access point configuration to protect CDE & CHD.
- Implement and update anti-virus software programs in systems and applications to detect and immediately remediate cyber-threats.
- Encrypt transmission of Cardholder Data across open, public networks to prevent unauthorized access of sensitive data.
- Develop and maintain secure systems and applications such as the Point-of-sale (POS) systems which include the payment terminals, cash registers, card readers, and other systems that intake payment card data from a customer at the time of a payment transaction.

- Track and monitor all access to network resources and Cardholder Data including web servers, application servers, database servers, authentication servers, mail servers, proxy servers, domain name servers, etc.
- Restrict physical access to Cardholder Data stored in the machines, applications, desktop networks, cloud.
- Regularly test security systems and processes to secure the Card Data Environment.
- Avoiding the use of vendor-supplied defaults for system passwords and other security parameters.

It is observed that most incidents of Data Breach that occur in the retail sector involve compromised Cardholder Data Environment. So, the PCI DSS requires the implementation of controls to secure the CDE. If the size and scope of the Cardholder Data Environment is minimum and adequately isolated by adopting proven techniques and advanced technology, it will reduce the likelihood and impact of a data breach.

How can the Cardholder Data Environment be secured and made PCI Compliant?

First and foremost Merchants and Service Providers are required to size and scope their Cardholder Data Environment to gauge their current risk exposure. Scoping and analyzing the Cardholder Data Environment will indicate the likelihood of their business facing incidents of data breaches. Depending on whether the Cardholder Data Environment (CDE) is minimal and adequately isolated or extensive, the systems, applications, and network accordingly fall in the scope of PCI DSS that needs to be secured. Given below is a technique that can help Merchants and Service Providers reduce the scope of PCI Compliance and also effectively secure their CDE.

Network Segmentation

It can be very challenging for the Merchants and Service Providers in the industry to ensure the Cardholder Data Environment is secure and PCI Compliant. In order to secure the CDE, organizations will need to adopt the process of Network Segmentation. This is to map the flow of the Cardholder Data and determine the scope for PCI Compliance. involves segmenting of data network into separate sections to isolate card data from all other computing processes. With this, it helps organizations gain better control over the flow of traffic across the network. Further, Network Segmentation helps restrict card data to a specific network segment and enables organizations to implement necessary controls for securing networks comprising Cardholder Data. This way, it enables organizations to minimize their scope of PCI DSS Compliance while also ensuring the security of the Cardholder Data Environment. Network Segmentation improves the security of the Cardholder Data and Cardholder Data Environment by making it easier for organizations to identify anomalies within their distinct network. With this, it reduces the overall chances of an organization encountering incidents of a Data Breach. Just to be clear, Network Segmentation is not a mandate under PCI DSS but is a recommendation.

Final Thought

The Security of Cardholder Data Environment and PCI DSS Compliance simply requires subject expertise. Since the security requirements in PCI DSS is not completely straightforward and requires an in-depth understanding of systems and network components, it is often recommended that organizations approach experts for guidance. With the right support of experienced and knowledgeable industry experts, the journey of Compliance and securing the CDE can be a lot easier

Original Source:- [Paymentsjournal]

Written By:- VISTA InfoSec

Do write to us your feedback, comments and queries or, if you have any requirements: info@vistainfosec.com

You can reach us on:

USA	INDIA	SINGAPORE	UK
+1-415-513 5261	+91 73045 57744	+65-3129-0397	+447405816761