Unit 5 Research Project

Eddie S. Jackson

Kaplan University

IT540: Management of Information Security

Kenneth L. Flick, Ph.D.

10/21/2014

Table of Contents

Abstract

The unit five research project delves into the topic of payment card industry (PCI). There are two parts of the research project that reinforce the twelve requirements of PCI specification. In part one of the assignment, a shopping scenario is presented where several products are paid for using a credit card. The entire payment process is to be assessed and associated with the relative PCI compliance standard. In part two of the research project, four questions are raised about PCI compliance in HGA's network. Using a given network diagram, HGA needs be evaluated for PCI compliancy, and suggestions must be made to increase security. Ultimately, the project is meant to build knowledge across a myriad of security subjects, including risk assessment of information systems, encryption, and physical security.

Unit 5 Research Project

Part I – PCI Scenario

In part one of the assignment, there is a visit to a local retail store. Several products are picked up and taken to a point of sale (POS) register system. The items are scanned and bagged, and then a credit card is used to pay for the products. The sales clerk completes the transaction and hands over a sales receipt. Upon exiting the store, a store employee asks for the sales receipt and verifies the purchased products. Using this scenario, different aspects of information systems are associated with the steps of the checkout process and explained in terms of PCI compliancy. PCI, or PCI DSS (Payment Card Industry Data Security Standard), refers to the policies and procedures that enhance security related to credit, debit, and cash cards (Rouse, n.d.).

PCI standard number eight. The initial step in the retail scenario is paying for the purchased items; this is when a credit card is swiped via a scanner. Before any transaction takes place, the sales clerk will need access to authorize the transaction; thus, the sales clerk must be logged into the POS system. According to the number eight PCI requirement–identify and authenticate access to system components–the sales clerk processing the transaction should have some kind of unique identification number or password for logging into the POS system (Whitman & Mattord, 2011). This POS information can be used to identify and track the sales clerk's authorization history, which is essential in maintaining system security. Once the transaction is entered, and the sales clerk authorizes the sale, the customer's data travels across a wire to a server. There are several PCI data standards associated with the transmission and processing of customer data.

PCI standard number four. First, the transmission itself must be secure; this applies to the fourth PCI standard, which is all cardholder data must be encrypted across open networks (Security Standards Council, 2014). One such method for securing the data stream across public

networks is implementing Secure Sockets Layer (SSL). SSL works by creating an encrypted communication link between the sender and receiver; in the retail scenario, the encrypted channel would be between the POS system and the credit card company (Digicert, n.d.).

PCI standard number one. Of course, there are other hardware components related to the transaction process. The retail store and credit card company should use some type of perimeter security, such as firewalls; this would relate to the number one PCI standard–installing and maintaining a firewall to protect customer data. Firewalls act as barriers between public and private networks, and provide multiple strategies for securing internal networks; for instance, access control lists (ACLs) can be created and managed to protect network resources at the store and the credit card company. ACLs work by defining which types of traffic are allowed, and which types are denied–thus acting as a network filter (Wilson, 2012). It is important to note, firewalls, routers, and some switches have ACL capability.

PCI standard number three. Perimeter security is critical to the protection of cardholder's data, but so is protecting the data while in storage or at rest; protecting this stored data refers to the PCI requirement number three. A best practice method for protecting cardholder data is to encrypt the hard drives. A popular encryption application that can protect stored data is Microsoft's Bitlocker. Bitlocker works by encrypting the whole hard drive, thus protecting the cardholder data in the case of physical theft of the servers or hard drives (Microsoft, n.d.). This segues into the next PCI standard, physical security.

PCI standard number nine. The ninth PCI specification requires physically securing the servers and network equipment that process cardholder transactions. By restricting access to the POS network equipment at the store, and the network resources located at the credit card company, cardholder data can be protected from theft. Physical security would include locking

doors, monitoring secured areas with cameras, and requiring digital badges to enter protected areas (USDA, n.d.).

In summary of the entire transaction process: the sale's clerk must have valid access to the POS system using unique credentials; the credit card data must securely traverse the network using SSL; perimeter security must be implemented via firewalls to protect the internal networks from public access; the cardholder data must be protected while in storage using encryption; and finally, there must be restricted access to network resources to protect the cardholder data from physical theft.

Part II – PCI Questions

In part two of the assignment, HGA's network is assessed for PCI compliancy using a network diagram. The HGA diagram is evaluated for potential security problems, as well as for areas that could benefit from enhanced security. Once the network diagram has been studied, there are four PCI-related questions that must be reviewed and security-based solutions provided. The questions include protecting private databases, securing data transmissions, implementing access controls, and reducing the scope of compliance.

Private databases. The first question concerns storing customer data in private databases. The question asks, "What steps should be taken to make sure the stored data is PCI compliant?" This question directly relates to the third PCI specification, protecting stored data. The third PCI specification deals with protecting data in the case of lost or stolen equipment. To guarantee that the private databases remain safe, even if they are stolen, it is suggested that the hard drives in the HGA mainframe be protected with full drive encryption. Full drive encryption is just how it sounds; it encrypts all the data on a specific hard drive. One popular full drive encryption software is Microsoft's Bitlocker Drive Encryption (BDE). BDE works by utilizing

an onboard microchip, a Trusted Platform Module (TPM) chip (Microsoft, n.d.). The TPM chip acts as a secure holding place to store cryptographic information. This cryptographic information is tamper-proof, and allows the chip to pass the correct key to the operating system during the boot process. If the operating system or BIOS has been tampered with, the key will not be passed, and the operating system enters a lockout status which requires a forty-eight digit key to be entered (Microsoft, n.d.). By implementing such encryption software, the HGA databases become PCI compliant.

Data transmissions. The next question asks, "What is the proper method for securely transmitting data across networks?" When considering the secure transmission of data, the relative PCI specification is number four. The fourth PCI requirement states that data must be encrypted across open or public networks. After reviewing the network HGA diagram, it is recommended that Secure Sockets Layer (SSL) be implemented on the HGA mainframe. SSL is a security protocol that was created for the specific purpose of establishing and maintaining an encrypted communication stream between a client and server (Digicert, n.d.). SSL works by connecting a client to a server; the server sends back a SSL certificate; the client checks to see if it trusts the server (from its certificate store); if the client trusts the server, a symmetric session key is sent back; once the server has the key, it is decrypted and an encrypted session is started (Digicert, n.d.). The SSL protocol is a well-known, secure method for protecting data while in transit; and thus, is required at HGA to meet the number four PCI specification.

Access controls. The third question is about restricting unauthorized users from accessing cardholder data. The PCI specification that relates to data access is number seven. The seventh PCI requirements states that access to cardholder data must be on a business need-to-know basis only. After reviewing HGA's network diagram, and factoring in that users are

located at various sites, the best solution to control access to cardholder data would be to install Microsoft's Active Directory. Active Directory is a type of database based upon the Lightweight Directory Access Protocol (LDAP) (Microsoft TechNet, n.d.). Active Directory's implementation of LDAP has the ability to replicate network related information from one domain controller to the next, even if those servers are geographically dispersed. This replication feature is particularly useful with administering security on files and folders throughout a network. The access controls themselves would be in the form of groups. Groups would be created and then user accounts added to them. The groups are associated with specific files and folders; anyone else that is not part of that group would not have access to open, view, or modify the cardholder data. Thus, implementing Active Directory, and using groups to control access to cardholder data, would allow HGA to meet the seventh PCI requirement.

Reducing scope of compliance. The last question is about reducing the scope of compliance. HGA has many devices connected to its network. Due to PCI compliancy, all these network resources must adhere to the strict guidelines of the PCI specifications. To reduce the administrative overhead of enforcing PCI compliance on all devices, it is recommended that non-essential services and servers be segmented. After reviewing the HGA network diagram, the best way to handle segmentation would be to use switches. Switches offer the unique ability to implement virtual LANs (VLANs). VLANs can segment a network by function, department, or even application (Cisco, n.d.); and thus, would provide a secure, cost effective way of logically separating the critical PCI compliance services and servers, from the non-critical services and servers.

References

Cisco. (n.d.). Configuring VLANs. Retrieved from http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/VLANs.html

Digicert. (n.d.). What is SSL (Secure Sockets Layer) and what are SSL certificates? Retrieved from https://www.digicert.com/ssl.htm

Microsoft. (n.d.). Bitlocker Drive Encryption. Retrieved from http://windows.microsoft.com/en-us/windows7/products/features/bitlocker

Microsoft. (n.d.). BitLocker Drive Encryption Overview. Retrieved from http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview

Microsoft TechNet. (n.d.). Active Directory. Retrieved from http://technet.microsoft.com/en-us/library/bb742424.aspx

Rouse, Margaret. (n.d.). PCI DSS (Payment Card Industry Data Security Standard). Retrieved from http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

Security Standards Council. (2014/8). PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.0. Retrieved from https://www.pcisecuritystandards.org/documents/PCISSC%20QRG%20August%202014%20-print.pdf

USDA. (n.d.). Security in the workplace - informational material. Retrieved from http://www.dm.usda.gov/physicalsecurity/workplace.htm

Whitman, Michael E., & Mattord, Herbert J. (2011). *Principles of Information Security*. 4th edition. Independence, KY: Cengage.

Wilson, Tracey. (2012/5/16). Securing networks: access control list (ACL) concepts. Retrieved from http://blog.pluralsight.com/access-control-list-concepts