Complying with PCI DSS&ndash;Part 3: Maintain a Vulnerability Management Program

Peter Silva, 2012-19-04

According to the PCI SSC, there are 12 PCI DSS requirements that satisfy a variety of security goals. Areas of focus include building and maintaining a secure network, protecting stored cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining information security policies. The essential framework of the PCI DSS encompasses assessment, remediation, and reporting. We're exploring how F5 can help organizations gain or maintain compliance and today is **Maintain a Vulnerability Management Program** which includes PCI Requirements 5 and 6. To read Part 1, click: Complying with PCI DSS–Part 1: Build and Maintain a Secure Network and Part 2: Complying with PCI DSS–Part 2: Protect Cardholder Data

Requirement 5: Use and regularly update antivirus software or programs.

PCI DSS Quick Reference Guide description: *Vulnerability management is the process of systematically and continuously finding weaknesses in an entity's payment card infrastructure system. This includes security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.*

Solution: With BIG-IP APM and BIG-IP Edge Gateway, F5 provides the ability to scan any remote device or internal system to ensure that an updated antivirus package is running prior to permitting a connection to the network. Once connections are made, BIG-IP APM and BIG-IP Edge Gateway continually monitor the user connections for a vulnerable state change, and if one is detected, can quarantine the user on the fly into a safe, secure, and isolated network. Remediation services can include a URL redirect to an antivirus update server. For application servers in the data center, BIG-IP products can communicate with existing network security and monitoring tools. If an application server is found to be vulnerable or compromised, that device can be automatically quarantined or removed from the service pool.

With BIG-IP ASM, file uploads can be extracted from requests and transferred over iCAP to a central antivirus (AV) scanner. If a file infection is detected, BIG-IP ASM will drop that request, making sure the file doesn't reach the web server.

Requirement 6: Develop and maintain secure systems and applications.

PCI DSS Quick Reference Guide description: *Security vulnerabilities in systems and applications may allow criminals to access PAN and other cardholder data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation. Entities should apply patches to less-critical systems as soon as possible, based on a risk-based vulnerability management program. Secure coding practices for developing applications, change control procedures, and other secure software development practices should always be followed.*

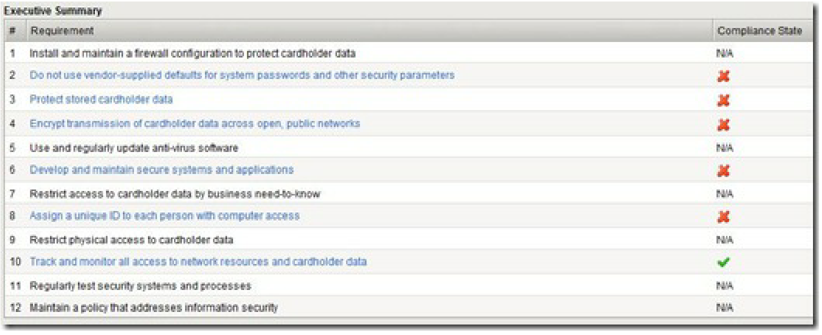
Solution: Requirements 6.1 through 6.5 deal with secure coding and application development; risk analysis, assessment, and mitigation; patching; and change control. Requirement 6.6 states: "*Ensure all public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications*."

This requirement can be easily met with BIG-IP ASM, which is a leading web application firewall (WAF) offering protection for vulnerable web applications. Using both a positive security model for dynamic application protection and a strong, signature-based negative security model, BIG-IP ASM provides application-layer protection against both targeted and generalized application attacks. It also protects against the Open Web Application Security Project (OWASP) Top Ten vulnerabilities and threats on the Web Application Security Consortium's (WASC) Threat Classification lists. To assess a web application's vulnerability, most organizations turn to a vulnerability scanner. The scanning schedule might depend on a change in control, as when an application is initially being deployed, or other triggers such as a quarterly report. The vulnerability scanner scours the web application, and in some cases actually attempts potential attacks, to generate a report indicating all possible vulnerabilities. This gives the administrator managing the web security devices a clear view of all exposed areas and potential threats to the website. Such a report is a moment-in time assessment and might not result in full application coverage, but should give administrators a clear picture of their web application security posture. It includes information about coding errors, weak authentication mechanisms, fields or parameters that query the database directly, or other vulnerabilities that provide unauthorized access to information, sensitive or not. Otherwise, many of these vulnerabilities would need to be manually re-coded or manually added to the WAF policy—both expensive undertakings.

Simply having the vulnerability report, while beneficial, doesn't make a web application secure. The real value of the report lies in how it enables an organization to determine the risk level and how best to mitigate the risk. Since recoding an application is expensive and time-consuming and may generate even more errors, many organizations deploy a WAF like BIG-IP ASM. A WAF enables an organization to protect its web applications by virtually patching the open vulnerabilities until developers have an opportunity to properly close the hole. Often, organizations use the vulnerability scanner report to either tighten or initially generate a WAF policy. While finding vulnerabilities helps organizations understand their exposure, they must also have the ability to quickly mitigate those vulnerabilities to greatly reduce the risk of application exploits. The longer an application remains vulnerable, the more likely it is to be compromised.

For cloud deployments, BIG-IP ASM Virtual Edition (VE) delivers the same functionality as the physical edition and helps companies maintain compliance, including compliance with PCI DSS, when they deploy applications in the cloud. If an application vulnerability is discovered, BIG-IP ASM VE can quickly be deployed in a cloud environment, enabling organizations to immediately patch vulnerabilities virtually until the development team can permanently fix the application. Additionally, organizations are often unable to fix applications developed by third parties, and this lack of control prevents many of them from considering cloud deployments. But with BIG-IP ASM VE, organizations have full control over securing their cloud infrastructure. BIG-IP ASM version 11.1 includes integration with IBM Rational AppScan, Cenzic Hailstorm, QualysGuard WAS, and WhiteHat Sentinel, making BIG-IP ASM the most advanced vulnerability assessment and application protection on the market. In addition, administrators can better create and enforce policies with information about attack patterns from a grouping of violations or otherwise correlated incidents. In this way, BIG-IP ASM protects the applications between scanning and patching cycles and against zero-day attacks that signature-based scanners won't find. Both are critical in creating a secure Application Delivery Network.

BIG-IP ASM also makes it easy to understand where organizations stand relative to PCI DSS compliance. With the BIG-IP ASM PCI Compliance Report, organizations can quickly see each security measure required to comply with PCI DSS 2.0 and understand which measures are or are not relevant to BIG-IP ASM functions. For relevant security measures, the report indicates whether the organization's BIG-IP ASM appliance complies with PCI DSS 2.0. For security measures that are not relevant to BIG-IP ASM, the report explains what action to take to achieve PCI DSS 2.0 compliance.



Executive Summary

#	Requirement	Compliance State
1	Install and maintain a firewall configuration to protect cardholder data	N/A
2	Do not use vendor-supplied defaults for system passwords and other security parameters	✗
3	Protect stored cardholder data	✗
4	Encrypt transmission of cardholder data across open, public networks	✗
5	Use and regularly update anti-virus software	N/A
6	Develop and maintain secure systems and applications	✗
7	Restrict access to cardholder data by business need-to-know	N/A
8	Assign a unique ID to each person with computer access	✗
9	Restrict physical access to cardholder data	N/A
10	Track and monitor all access to network resources and cardholder data	✓
11	Regularly test security systems and processes	N/A
12	Maintain a policy that addresses information security	N/A

BIG-IP ASM PCI Compliance Report

Finally, with the unique F5 iHealth system, organizations can analyze the configuration of their BIG-IP products to identify any critical patches or security updates that may be necessary.

Next: Implement Strong Access Control Measures

ps

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com