Complying with PCI DSS–Part 5: Regularly Monitor and Test Networks

Peter Silva, 2012-24-04

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 Regularly Monitor and Test Networks which includes PCI Requirements 10 and 11. To read Part 1, click: Complying with PCI DSS–Part 1: Build and Maintain a Secure Network, Part 2:Complying with PCI DSS–Part 2: Protect Cardholder Data, Part 3: Complying with PCI DSS–Part 3: Maintain a Vulnerability Management Program and Part 4: Complying with PCI DSS–Part 4: Implement Strong Access Control Measures.

Requirement 10: Track and monitor all access to network resources and cardholder data.

PCI DSS Quick Reference Guide description: *Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is very difficult without system activity logs.*

Solution: The spirit of this requirement is to ensure appropriate systems generate logs, with implementation and monitoring of log aggregation and correlation systems. The ability to monitor and log all user sessions and requests for access to sensitive information, such as cardholder data and Social Security numbers, is critical to any security environment. F5 offers a suite of solutions that are session-based, not packet-based. With this full reverse proxy architecture, the BIG-IP platform has the ability to manage full user sessions, regardless of the transport mechanism or network, and match those user sessions to specific data actions, supplying log data and a full audit trail from the user to the data. This allows F5 application security devices to ensure the confidentiality, integrity, and availability of all application data on the network.

All F5 products support remote logging, allowing logs to be pushed to secure networks and devices for archiving. In addition, the TMOS architecture can manage isolated, secure logging networks in conjunction with the application networks, using features such as mirrored ports, VLANs, and virtualized administrative access. Protecting network resources and application data 24 hours a day, seven days a week, without affecting network performance, is a core function and the foundation of all F5 security products.

Requirement 11: Regularly test security systems and processes.

PCI DSS Quick Reference Guide description: *Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security is maintained over time. Testing of security controls is especially important for any environmental changes such as deploying new software or changing system configuration.*

Solution: The spirit of this requirement is to ensure that the complying organization itself tests its security system and processes. Since F5 does not offer a penetration testing service, this is one of just two PCI DSS requirements that F5 products cannot significantly address.

Next: Maintain an Information Security Policy

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