|  |  |
| --- | --- |
| **5.2** Ensure that all anti-virus mechanisms are maintained as follows:   * Are kept current. * Perform periodic scans. * Generate audit logs which are retained per PCI DSS Requirement 10.7. | |
| **5.2.d** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that:   * *Anti-virus software log generation is enabled, and;* * *Logs are retained in accordance with PCI DSS Requirement 10.7.* | **Identify the sample** of system components selected for this testing procedure. |
| *For each item in the sample,* **describe how** anti-virus configurations, including the master installation of the software, verified that: |
| * Anti-virus software log generation is enabled, and; |
| * Logs are retained in accordance with PCI DSS Requirement 10.7. |

# Breakdown of Existing DSS Logging & Alerting (Non-Server)

|  |  |
| --- | --- |
| Validation Summary: | For each relevant system ensure that the anti-malware mechanism is logging (centrally or locally). If locally, ensure that there is sufficient disk space to store 1 year’s worth of logs.  Requirement 10.2.3 will apply.  Requirements 10.5.1, 10.5.2, 10.5.3 and 10.5.5 will apply.  Requirement 10.6.x will apply. |
| Log Centralisation: | Not required, but 10.5.3 applies. |
| Log Review: | Not specified, but 10.6.1 (or 10.6.2) and 10.6.3 should apply. |
| Event Alerting: | Not required. |
| Incident Response: | Not specified, but 12.10.1 applies. |

|  |
| --- |
| **6.6** For *public-facing* web applications, ensure that *either one* of the following methods is in place as follows:   * Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: * At least annually. * After any changes. * By an organization that specializes in application security. * That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment. * That all vulnerabilities are corrected. * That the application is re-evaluated after the corrections. * Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: * Is situated in front of public-facing web applications to detect and prevent web-based attacks. * Is actively running and up-to-date as applicable. * *Is generating audit logs.* * Is configured to either block web-based attacks, or generate an alert that is immediately investigated. |

|  |  |
| --- | --- |
| Validation Summary: | IF an “automated technical solution that detects and prevents web-based attacks” is in use, ensure that it is logging (centrally or locally). If locally, ensure that there is sufficient disk space to store 1 year’s worth of logs.  Requirement 10.2.3 will apply.  Requirements 10.5.1, 10.5.2, 10.5.3 and 10.5.5 will apply. |
| Log Centralisation: | Not required, but 10.5.3 applies. |
| Log Review: | Not specified, but 10.6.1 and 10.6.3 should apply. |
| Event Alerting: | Not required. |
| Incident Response: | Not specified, but 12.10.1 applies. |

|  |  |
| --- | --- |
| **11.1** Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. | |
| **11.1.d** If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), *verify the configuration will generate alerts to notify personnel*. | * *For each monitoring technology in use,* **describe how** the technology generates alerts to personnel. |

|  |  |
| --- | --- |
| Validation Summary: | IF “automated monitoring” for wireless access points is in use, ensure that it generates alerts.  Logging has not been specified, so:  Requirement 10.2.3 does not apply.  Requirements 10.5.1, 10.5.2, 10.5.3 and 10.5.5 do not apply. |
| Log Centralisation: | Not required. |
| Log Review: | Not required. |
| Event Alerting: | Required, but no definition of time-frame. |
| Incident Response: | Not specified, but 12.10.1 applies. |

|  |  |
| --- | --- |
| **11.4** Use intrusion-detection systems and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date. | |
| **11.4.b** Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques *alert personnel of suspected compromises*. | **Describe how** system configurations for intrusion-detection and/or intrusion-prevention techniques verified that they are configured to alert personnel of suspected compromises. |
| * Identify the responsible personnel interviewed who confirm that the generated alerts are received as intended. |
| **11.4.c** Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection, and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection. | **Describe how** IDS/IPS configurations and vendor documentation verified that intrusion-detection, and/or intrusion-prevention techniques are: |
| * Configured per vendor instructions to ensure optimal protection. |
| * Maintained per vendor instructions to ensure optimal protection. |
| * Updated per vendor instructions to ensure optimal protection. |

|  |  |
| --- | --- |
| Validation Summary: | Confirm that IDS at a minimum is installed within the CDE. Nothing in the language precludes a manual review of the results.  Requirement 10.2.3 will apply to the scan results.  Requirements 10.5.1, 10.5.2, 10.5.3 and 10.5.5 will apply to the scan results. |
| Log Centralisation: | Not required. |
| Log Review: | Not specified, but 10.6.1 and 10.6.3 should apply. |
| Event Alerting: | Required, but no definition of time-frame. “Generated alerts” does not mean by the IDS itself [necessarily], nor does it mandate that alerts must be generated *automatically*. |
| Incident Response: | 12.10.1 fully applies. |

|  |  |
| --- | --- |
| **11.5.a** Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored:  • System executables  • Application executables  • Configuration and parameter files  • Centrally stored, historical or archived, log and audit files  • Additional critical files determined by entity (i.e., through risk assessment or other means) | **Identify the results** from monitored files reviewed to verify the use of a change-detection mechanism. |
| **11.5.b** Verify the mechanism is configured to *alert personnel to unauthorized modification* (including changes, additions and deletions) of critical files, and to perform critical file comparisons at least weekly. | **Describe how** system settings verified that the change-detection mechanism is configured to: |
| * Alert personnel to unauthorized modification (including changes, additions and deletions) of critical files. |
| **11.5.1** Implement a process to respond to any alerts generated by the change-detection solution. | N/A |

|  |  |
| --- | --- |
| Validation Summary: | Confirm that all relevant files are compared weekly and that alerts are generated in some fashion. Nothing in the language precludes a manual review of the comparison results.  Requirement 10.2.3 will apply to the comparison results.  Requirements 10.5.1, 10.5.2, 10.5.3 and 10.5.5 will apply to the comparison results. |
| Log Centralisation: | Not required. |
| Log Review: | Required on a weekly basis. |
| Event Alerting: | Required, but no definition of time-frame, or whether the alert must be generated automatically. |
| Incident Response: | 12.10.1 fully applies. |

# Missing from the DSS

## DSS Requirements 1.x: Review of traffic logs from firewalls and routers

With regard firewalls and routers, the PCI DSS 10.2.x requirements relate entirely to administrative access to the systems, and not to functionality of the devices themselves.

Through base-lining and automated review, the traffic logs from network devices can provide significant input to the security posture of other devices.

*Examination of Network Device Traffic:*

|  |  |
| --- | --- |
| **1.1.1.c** Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested. | Any change to a firewall/router ruleset should generate an alert, or be automatically compared to open change control tickets. |
| **1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each. | Network devices should deny any protocols not specifically allowed, therefore ANY denies between internal systems denote a server misconfiguration. |
| **1.2.1.b** Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment. | Network devices should deny any traffic not specifically allowed, therefore ANY denies to or from in-scope systems denote a server misconfiguration. |
| **1.3.2** Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ. | Any outbound requests to IPs NOT in the DMZ should be investigated. |
| **1.3.4** Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. | ANY outbound denies from in-scope systems should generate an alert |

*DSS Requirements 2.X: Review of server configuration settings.*

With proper asset management system (AMS) in place and a simple host-based agent, a significant number of automated alerts can be configured.

The ASM would need to record these attributes against each server asset:

1. All available services
2. All listening ports
3. Established connections

The ASM would need to define corporate policies and standards (e.g. for permitted protocols)

*Examination of server logs:*

|  |  |
| --- | --- |
| **2.2.1.a** Select a sample of system components and inspect the system configurations to verify that only one primary function is implemented per server. | Centralised policy management through the AMS will denote what security level is applied to each function (defined by running services and listening ports). Alerts can be generated when ‘high’ and ‘low’ security levels are detected on the same system. |
| **2.2.2.a** Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled. | Each server will have a ‘known-good’ profile maintained in the AMS that will include;   1. List of all available services 2. List of all listening ports 3. List of all approved established connections   All services and ports should be defined in a global policy.  Automated comparisons against system settings obtained from local agents should generate an alert if anything changes, or if anything is outside of policy. |
| **2.2.2.b** Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards. |
| **2.2.5.a** Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. | Each server will have a ‘known-good’ profile maintained in the AMS that will include;   1. List of all available services 2. List of all listening ports 3. List of all approved established connections   All services and ports should be defined in a global policy.  Automated comparisons against system settings obtained from local agents should generate an alert if anything changes, or if anything is outside of policy. |
| **2.2.5.b** Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration. |
| **2.3.b** Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access. | All insecure services should be defined and prohibited in global policy, so any use of the service will generate an alert automatically. |
| **2.4.a** Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each. | Asset Management System. |

*DSS Requirements 3.X: Unencrypted cardholder data / sensitive authentication data.*

Requires host-based DLP agent.

*Examination of system files and logs:*

|  |  |
| --- | --- |
| **3.2.c** For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization. | Host-based agent capable of DLP functionality sends automated alerts either directly, or via centralised management station (e.g. a SIEM). |
| **3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents |
| **3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents |  |
| **3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization:   * Incoming transaction data * All logs (for example, transaction, history, debugging, error) * History files * Trace files * Several database schemas * Database contents |

*DSS Requirements 4.X: Unencrypted email.*

Requires email or perimeter based DLP.

*Examination of server logs:*

|  |  |
| --- | --- |
| **4.2.a** If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. | Email or perimeter based DLP will detect and potentially stop incoming and outgoing emails containing cardholder data. |

*DSS Requirements 5.X: Anti-Malware.*

Requires centralised management station capable of generating alerts.

*Examination of server logs:*

|  |  |
| --- | --- |
| **5.2.d** Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that:   * Anti-virus software log generation is enabled, and * Logs are retained in accordance with PCI DSS Requirement 10.7. | Any detection of malware should at a minimum create an alert, but automatic quarantining is preferred along with the alert. |

*DSS Requirements 6.X: Patch Management.*

Requires centralised policy manager and host-based agent to allow for automated comparison of installed patches vs. approved policy and baseline configs.

*Examination of server logs:*

|  |  |
| --- | --- |
| **6.2.b** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following:   * That applicable critical vendor-supplied security patches are installed within one month of release. * All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). | Any detection of malware should at a minimum create an alert, but automatic quarantining is preferred along with the alert. |

*DSS Requirements 7.X: Access Control.*

Requires centralised policy manager and host-based agent to allow for automated comparison of access control settings (e.g. local access vs GPO assignments for Windows).

*Examination of server logs:*

|  |  |
| --- | --- |
| **7.2.1** Confirm that access control systems are in place on all system components. | Any detection of access methods outside of approved policy should create an alert. E.g. ‘Guest’ access, or ‘Local’ access outside of the established GPO. |

*DSS Requirements 8.X: Password Settings.*

Requires centralised policy manager and host-based agent to allow for automated comparison of access control settings (e.g. password complexity minimums).

*Examination of server logs:*

|  |  |
| --- | --- |
| **8.1.4** Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled. | Any detection of authentication methods outside of approved policy should create an alert. |
| **8.1.6.a** For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts. |
| **8.1.7** For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. |
| **8.1.8** For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. |
| **8.2.3.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require at least the following strength/complexity:   * Require a minimum length of at least seven characters. * Contain both numeric and alphabetic characters. |
| **8.2.4.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require users to change passwords/passphrases at least once every 90 days. |
| **8.2.5.a** For a sample of system components, obtain and inspect system configuration settings to verify that password/passphrases parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases. |
| **8.2.6** Examine password procedures and observe security personnel to verify that first-time passwords/passphrases for new users, and reset passwords/passphrases for existing users, are set to a unique value for each user and changed after first use. |

# Automating The ‘Daily’ Review

It is possible to replace the daily review with the following 3 things, but it will require either a rudimentary SIEM, or s scripting skills:

1. The Never-See Events – every system administrator (OS, application. DB etc.) should be able to determine which events should NEVER be seen during the normal running of their systems (e.g. for a Windows Admin ‘Event ID 1100 The event logging service has shut down’ should never be seen under normal conditions).
2. Threshold Events – This is where a single may not be an issue, but a certain number in a specific timeframe might be (e.g. a single failed logon is probably irrelevant, but 5 in 1 second is not).
3. Trending Events – PCI requires you to keep a year’s worth of logs, so you may as well do something with them. By base-lining the number of events received from a system to time of day, day of the week, and ‘peak’ times, significant variations can be determined (e.g. a server that normally logs only a few events between the hours of 7PM and 8AM suddenly see a spike, may be worth investigating).