Kaspersky®
Embedded Systems
Security

PCI DSS v3.2 Mapping

PCI DSS 3.2 regulates many technical security requirements and settings for systems operating with credit card data. Sub-points 1.4, 2.4a, 5.1, 5.1.1, 5.2, 5.3, 6.2, 10.5.5, 11.5 of PCI DSS v3.2 provide for the strict regulation of antivirus protection relating to any endpoint which is operating with Cardholder Details Data. It is common practice, though not an official rule, for Device Control + Application Control functions to be considered as also within the remit of the PCI DSS antivirus software audit.

1.4

PCI DSS REQUIREMENTS:

Install personal firewall software or equivalent functionality on any portable computing devices that connect to the Internet when outside the network, and which are also used to access the CDE. Firewall (or equivalent) configurations include:

- Specific configuration settings are defined.
- Personal firewall (or equivalent functionality) is actively running.
- Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.

TESTING PROCEDURES:

1.4.a Examine policies and configuration standards to verify:

- Personal firewall software or equivalent functionality is required for all portable computing devices that connect to the Internet when outside the network, and which are also used to access the CDE.
- Specific configuration settings are defined for personal firewall (or equivalent functionality).
- Personal firewall (or equivalent functionality) is configured to actively run.
- Personal firewall (or equivalent functionality) is configured to not be alterable by users of the portable computing devices.

1.4.b Inspect a sample of company devices to verify that:

- Personal firewall (or equivalent functionality) is installed and configured per the organization's specific configuration settings.
- Personal firewall (or equivalent functionality) is actively running.
- Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.

GUIDANCE:

Portable computing devices that are allowed to connect to the Internet from outside the corporate firewall are more vulnerable to Internet-based threats. Use of firewall functionality (e.g., personal firewall software or hardware) helps to protect devices from Internet-based attacks, which could use the device to gain access the organization's systems and data once the device is re-connected to the network.

The specific firewall configuration settings are determined by the organization.

2.4a

PCI DSS REQUIREMENTS	Maintain an inventory of system components that are in scope for PCI DSS.
TESTING PROCEDURES	**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.
GUIDANCE	Maintaining a current list of all system components will enable an organization to accurately and efficiently define the scope of their environment for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from the organization's configuration standards.

5.1

PCI DSS REQUIREMENTS:	Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).
TESTING PROCEDURES:	For a sample of system components including all operating system types commonly affected by malicious software, verify that antivirus software is deployed if applicable antivirus technology exists.
GUIDANCE:	There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. Without an antivirus solution that is updated regularly, these new forms of malicious software can attack systems, disable a network, or lead to compromise of data.

5.1.1

PCI DSS REQUIREMENTS:	Ensure that antivirus programs are capable of detecting, removing, and protecting against all known types of malicious software.
TESTING PROCEDURES:	Review vendor documentation and examine antivirus configurations to verify that antivirus programs detect all known types of malicious software, remove all known types of malicious software, and protect against all known types of malicious software.
GUIDANCE:	It is important to protect against ALL types and forms of malicious software.

5.2

PCI DSS REQUIREMENTS: Ensure that all antivirus mechanisms are kept current, perform periodic scans, and generate audit logs which are retained per PCI DSS Requirement 10.7.

TESTING PROCEDURES:

5.2.a Examine policies and procedures to verify that antivirus software and definitions are required to be kept up to date.

5.2.b Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are configured to perform automatic updates, and to perform periodic scans.

5.2.c Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that the antivirus software and definitions are current and periodic scans are performed.

5.2.d Examine antivirus 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.

GUIDANCE: Even the best antivirus solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections. Audit logs provide the ability to monitor virus and malware activity and antimalware reactions. Thus, it is imperative that antimalware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.

5.3

PCI DSS REQUIREMENTS: Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-bycase basis for a limited time period.

TESTING PROCEDURES:

5.3.a Examine antivirus configurations, including the master installation of the software and a sample of system components, to verify the antivirus software is actively running.

5.3.b Examine antivirus configurations, including the master installation of the software and a sample of system components, to verify that the antivirus software cannot be disabled or altered by users.

5.3.c Interview responsible personnel and observe processes to verify that antivirus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

GUIDANCE: Anti-virus that continually runs and is unable to be altered will provide persistent security against malware.

Use of policy-based controls on all systems to ensure anti-malware protections cannot be altered or disabled will help prevent system weaknesses from being exploited by malicious software.

Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active – for example, disconnecting the unprotected system from the Internet while the antivirus protection is disabled, and running a full scan after it is re-enabled.

6.2

PCI DSS REQUIREMENTS:

Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release

Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.

TESTING PROCEDURES:

6.2.a Examine policies and procedures related to security-patch installation to verify processes are defined for installation of applicable critical vendorsupplied security patches within one month of release, installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).

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 securitypatch list, to verify that applicable critical vendorsupplied security patches are installed within one month of release and all applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months).

GUIDANCE:

There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. If the most recent patches are not implemented on critical systems as soon as possible, a malicious individual can use these exploits to attack or disable a system, or gain access to sensitive data.

Prioritizing patches for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months.

This requirement applies to applicable patches for all installed software.

10.5.5

PCI DSS REQUIREMENTS:

Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

TESTING PROCEDURES:

Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.

GUIDANCE:

File-integrity monitoring or change-detection systems check for changes to critical files, and notify when such changes are noted. For file-integrity monitoring purposes, an entity usually monitors files that don't regularly change, but when changed indicate a possible compromise.

11.5

PCI DSS REQUIREMENTS:

Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

TESTING PROCEDURES:

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 (for example, through risk assessment or other means).

GUIDANCE:

Change-detection solutions such as file-integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected. If not implemented properly and the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing.