kaspersky BRING ON THE FUTURE

PCI DSS v3.2 Mapping

Kaspersky Embedded System Security

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 protection relating to any endpoint which is operating with cardholder data. It is common practice, although not an official rule, for Device Control + Application Control functions to also be considered to be within the remit of the PCI DSS antivirus software audit. More regulations covered by a single product makes compliance easier to achieve.

Kaspersky Embedded Systems Security covers a wide range of requirements:

1.4 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.

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.

5.1 Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).

5.1.1 Ensure that antivirus programs are capable of detecting, removing, and protecting against all known types of malicious software

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

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

6.2 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.*

10.5.5 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).

11.5 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.

*** Additional license required.**

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tommorow.

Know more at kaspersky.com/transparency

Proven. Transparent. Independent.