**How to Comply to Requirement 5 of PCI DSS**

The 12 PCI DSS requirements are laid down under the umbrella of 6 control objectives, with each requirement having a set of further sub-requirements. Requirement 5 and 6 are related to the maintenance of a vulnerability management program.

**Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.**

Malicious software or malware can easily enter an organizational network with simple organizational functions such as internet usage, employee emails, storage hardware, etc. Malware includes different types of viruses, Trojans, worms, spyware, rootkits, adware, etc., which can be used to exploit vulnerabilities in the system. For this reason, anti-virus software must be installed on every system to protect it against malware threats. This software needs to be kept updated regularly as new threats and viruses keep on emerging every day.

|  |  |
| --- | --- |
| **Malware Name** | **Description** |
| Macro Virus | These viruses are mostly found in Microsoft applications. They get attached to the initialization sequence of an application and replicate themselves. Whenever the application is opened, they attach themselves to other areas of the network or the system. |
| Worm | Worms replicate within an entire network and do not necessarily need to attach themselves with an application to do so. |
| Trojan Horse | Trojans do not replicate but create vulnerabilities in a network or a system by installing a “backdoor program”. |
| File Infector | These viruses are found mostly in .exe files. When such files are opened, the virus replicates itself and gets attached to other areas of the system or network. |
| Stealth Virus | These viruses are the most dangerous as they trick anti-virus software by falsely presenting an infected file as clean. |

.

**5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).**

Even secured systems face regular attacks as new vulnerabilities are discovered and new viruses keep on evolving. If the anti-virus is not regularly updated, these malware entities can attack and exploit a system to extract important data. Compliance to this requirement should be achieved by taking a sample of system components and verifying that an updated version of antivirus is deployed and fully functional.

Once the deployment of anti-virus software is verified, they need to be tested for detection, removal and protection against even the latest of the malwares.

Mid range and mainframe computers are normally not targetted by malware nowadays. Even then, new threats keep on emerging daily and industry trends can change anytime. It is therefore recommended to stay updated with new threats and take proactive measures in case of potential threats to such systems. Personnel should be interviewed for monitoring of such systems and any new malicious software trends should be communicated so that proper protection mechanisms can be implemented.

Intrusion detection systems have thus gained more importance as they do not require regular patches as opposed to anti-virus software which requires regular patching. Another advantage of such systems is that they can be installed on systems as well as network. These prevention systems should be installed before devices that hold cardholder data in order to make sure that maximum protection is provided. If you are using anti-virus software instead of intrusion detection system, make sure that your software is patched by comparing the total number of connected devices with those being updated. The Network Access Control (NAC) mechanism can also help to verify that all individual systems have latest patches applied to them.

**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.**

It is very important that all anti-virus software should be regularly updated to avoid the compromise of data through an unaddressed threat. If it is not updated regularly, even a very effective anti-virus can no more prove efficient as it is not updated with the knowledge of new viruses. Audit logs are also helpful as they aid in monitoring the virus and/or malware activity and the response of the anti-virus or anti-malware. Hence, audit logs must be enabled and managed according to the requirement 10 of the PCI DSS.

To achieve compliance, the following measures need to be taken:

* Check up the policies and procedures of the organization to make sure that they mention the need of updated antivirus software and confirm that it is applied according to the policies and procedures.
* Inspect the anti-virus configuration to verify that anti-virus scans are set to start automatically after certain time periods and are on auto-update mode.
* Verify by checking the anti-virus configuration, that log generation of anti-virus is enabled and are in compliance with requirement 10.7

**5.3 Ensure that anti-virus 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.**

Anti-virus should be set up in such a manner that its settings cannot be disabled or changed by any user, except the authorized personnel. When an anti-virus program runs continuously in the background, it can detect a virus in real time and will constantly check for malware threats. A strict policy prohibiting the alteration or disablement of the anti-virus should be communicated to the staff to stop any weaknesses from potential exploitation.

If the anti-virus is disabled for some amount of time due to any reasons, extra security measures should be taken such as, disabling internet connection before disabling anti-virus, and then performing a system scan after enabling it again. If an anti-virus program needs to be disabled because of any technical reasons, permission must be taken by the authority.

To ensure that all systems are complying with this requirement, examine a sample of systems and verify that all of them have their anti-virus programs running in real time. Also verify that none of the anti-virus programs of the taken sample can be disabled or altered by common users and that only personnel authorized by the management can make these changes in special case scenarios.

**5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.**

To make sure that every individual is aware of security policies and operational procedures of an organization, and to ensure maximum protection of the network from malware, personnel should be communicated the organizational policies and procedures regarding malware protection. To ensure compliance, this documentation should be regularly reviewed and staff should be ensured to verify their security awareness.