DMZ Configuration and Internet Access to the Cardholder Data Environment Policy

Overview

In accordance with the Payment Card Industry Data Security Standards (PCI DSS) requirements, The Office of Information Security has established a formal policy and supporting procedures concerning DMZ configuration and Internet access to the cardholder data environment. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

The Office of Information Security will ensure that the DMZ configuration and Internet access to the cardholder data environment policy adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Prohibit direct public access between the Internet and any system component in the cardholder data environment. (Req. 1.3).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that there is no direct access between the Internet and system components in the internal cardholder network segments. (Req. 1.3).
- Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. (Req. 1.3.1).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. (Req. 1.3.1).
- Limit inbound Internet traffic to IP addresses within the DMZ. (Req. 1.3.2).

- Appropriately configure, examine, and confirm firewall and router configurations to ensure that inbound Internet traffic is limited to IP addresses within the DMZ. (Req. 1.3.2).
- Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. (Req. 1.3.3).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment. (Req. 1.3.3).
- Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (Req. 1.3.4).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ. (Req. 1.3.4).
- Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. (Req. 1.3.5).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that outbound traffic from the cardholder data environment to the Internet is explicitly authorized. (Req. 1.3.5)
- Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.) (Req. 1.3.6).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that the firewall performs stateful inspection (dynamic packet filtering). (Req. 1.3.6).
- Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. (Req. 1.3.7).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks. (Req. 1.3.7).

- Do not disclose private IP addresses and routing information to unauthorized parties. (Req. 1.3.8).
- Appropriately configure, examine, and confirm firewall and router configurations to ensure that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. (Req. 1.3.8.a).
- Appropriately configure, examine, and confirm all applicable and necessary documentation to ensure that any disclosure of private IP addresses and routing information to external entities is authorized. (Req. 1.3.8.b).

The exposure of cardholder data environment system components to direct public Internet access poses obvious security risks by allowing untrusted parties to make direct connections to an environment containing privileged information. The prohibition of direct public Internet access to system components within cardholder data environments helps to ensure that sensitive data, as well as the architecture where sensitive data resides, are insulated from external threats seeking to exploit information or resources.

Responsibility for Policy Maintenance

The Office of Information Security is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

Revision History

February 8, 2019 (Policy Created)

July 15, 2019 (Policy Modified)

Adapted from Stanford University's PCI DSS Policies 1-2019