Requirement #11: Regularly Test Security Systems & Processes

Vulnerabilities are being discovered continually by malicious individuals and are being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect the changing environment.

PCI DSS Control 11.1

Control Objective: The organization implements processes to test for the presence of Wireless Access Points (WAPs) and detect and identify all authorized and unauthorized wireless access points.

Standard: Asset custodians are required to implement a process to test for the presence of Wireless Access Points (WAPs) that includes: [202]

(c) Detecting and identifying all authorized and unauthorized wireless access points at least once every ninety (90) days;
(d) Maintaining an inventory of authorized WAPs including a documented business justification; [203] and
(e) Implementing incident response procedures in the event unauthorized WAPs are detected. [204]

Supplemental Guidance: Detection methods must be sufficient to detect and identify both authorized and unauthorized devices. Methods that may be used in the rogue WAPs (802.11) detection process includes, but are not limited to:

- Wireless network scans,
- Physical/logical inspections of system components and infrastructure,
- Network Access Control (NAC); or
- Wireless Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)

Procedures: The City's wireless access points detect rogue access points, and the WLAN controller alerts IT via email.

PCI DSS Control 11.2

Control Objective: The organization implements a process for running internal and external network vulnerability scans at least quarterly and after any significant change in the network.

Standard: Asset custodians and data owners are required to perform the following vulnerability scanning-related activities: [205]

(a) Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel;[206]
(b) Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved; [207] and
(c) Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. [208]

Supplemental Guidance: A "quarter" is defined as a ninety (90) day period and a "significant change" in the network includes, but is not limited to:

- New system component installations;
- Changes in network topology;
- Firewall rule modifications; and
- Major product upgrades.

Procedures: Vulnerability scans are performed weekly. See the Vulnerability and Patch Management Program document for more details.

PCI DSS Control 11.3

Control Objective: The organization implements a methodology for penetration testing.

---

[202] PCI DSS v3.2 Requirement 11.1
[203] PCI DSS v3.2 Requirement 11.1.1
[204] PCI DSS v3.2 Requirement 11.1.2
[205] PCI DSS v3.2 Requirement 11.2
[206] PCI DSS v3.2 Requirement 11.2.1
[207] PCI DSS v3.2 Requirement 11.2.2
[208] PCI DSS v3.2 Requirement 11.2.3

Standard: Asset custodians and data owners are required to implement a methodology for penetration testing that includes the following:

(a) Coverage of all PCI DSS version 3.0 requirements: [209]
    1. Process is based on industry-accepted penetration testing approaches (e.g., NIST SP 800-115);
    2. Includes coverage for the entire CDE perimeter and critical systems;
    3. Includes testing from both inside and outside the network;
    4. Includes testing to validate any segmentation and scope-reduction controls;
    5. Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in PCI DSS requirement 6.5;
    6. Defines network-layer penetration tests to include components that support network functions, as well as operating systems;
    7. Includes review and consideration of threats and vulnerabilities experienced in the last twelve (12) months; and
    8. Specifies retention of penetration testing results and remediation activities results.
(b) External penetration testing must be performed at least annually and after any significant infrastructure or application upgrade or modification. Examples include, but are not limited to: [210]
    1. An operating system upgrade;
    2. A sub-network added to the environment; or
    3. A web server added to the CDE;
(c) Internal penetration testing must be performed at least annually and after any significant infrastructure or application upgrade or modification. Examples include, but are not limited to: [211]
    1. An operating system upgrade;
    2. A sub-network added to the environment; or
    3. A web server added to the CDE;
(d) Exploitable vulnerabilities found during penetration testing must be corrected and testing shall be repeated to verify the corrections; [212] and
(e) If segmentation is used to isolate the CDE from other networks, penetration tests must be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. [213]

Supplemental Guidance: This update to PCI DSS requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until v3.0 is in place.

Procedures: Penetration tests are performed annually. See the Vulnerability and Patch Management Program document for more details.

PCI DSS Control 11.4

Control Objective: The organization utilizes intrusion-detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network.

Standard: Asset custodians and data owners are required to utilize Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) to: [214]

(a) Prevent intrusions into the CDE;
(b) Monitor all traffic at the perimeter of the CDE, as well as at critical points in the CDE;
(c) Alert personnel to suspected compromises within the CDE; and
(d) Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.

Supplemental Guidance: Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known “signatures” and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection,

[209] PCI DSS v3.2 Requirement 11.3
[210] PCI DSS v3.2 Requirement 11.3.1
[211] PCI DSS v3.2 Requirement 11.3.2
[212] PCI DSS v3.2 Requirement 11.3.3
[213] PCI DSS v3.2 Requirement 11.3.4 & 11.3.4.1
[214] PCI DSS v3.2 Requirement 11.4

attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.

Procedures: The City's security fabric delivers broad protection and visibility to every network segment, device, appliance, whether virtual or physical. Both IDS and IPS are incorporated in the security fabric.

PCI DSS Control 11.5

Control Objective: The organization deploys change-detection mechanisms to alert personnel to unauthorized modifications.

Standard: Asset custodians and data owners are required to deploy a change-detection mechanism (e.g., File Integrity Monitoring (FIM) tools) to: [215]

(a) Alert personnel to unauthorized modification of:
   1. Critical system files;
   2. Configuration files; or
   3. Content files;

(b) Configure the change-detection mechanism software to perform file comparisons at least weekly; and

(c) Implement a process to respond to any alerts generated by the change-detection mechanisms. [216]

Supplemental Guidance: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).
Examples of files that should be monitored:

- System executables;
- Application executables;
- Configuration and parameter files; and
- Centrally stored, historical or archived, log and audit files.

Procedures: The City uses several different products to accomplish this: Stealthbits, NetMon, and ADManager.

PCI DSS Control 11.6

Control Objective: The organization ensures that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for security monitoring and testing are kept current and disseminated to all pertinent parties. [217]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures for security monitoring and testing on a continuous basis.

Procedures: Policies are emailed and posted to the City's Intranet site.

[215] PCI DSS v3.2 Requirement 11.5
[216] PCI DSS v3.2 Requirement 11.5.1
[217] PCI DSS v3.2 Requirement 11.6