29.01.03.H0.15 Vulnerability Assessment

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

Network scanning is frequently used in an attempt to gain a comprehensive network security report, detailing possible vulnerabilities of the systems attached. Additionally, all operating systems and applications for all information resource systems must undergo a regular vulnerability assessment as required by Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202, Subchapter C, Rule §202.75.

Applicability

This procedure applies to all users and administrators of Texas A&M University-Texarkana (TAMUT) Information Resources. It establishes guidelines on network scanning, vulnerability assessments of network systems, operating systems, and applications and specifies the roles of individuals who are authorized to perform network scans on TAMUT's network.

Definitions

Information Resources Manager (IRM): Person responsible to the State of Texas for management of the agency's information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the agency's information activities, and ensure greater visibility of such activities within and between State agencies. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards and guidelines to protect the Information Resources of the agency. At TAMUT, the IRM is the Associate Vice President for IT/CIO.

Information Security Officer (ISO): Person responsible to the executive management for administering the information security functions within the University. The ISO is TAMUT's internal and external point of contact for all information security matters.

Network Scanning: The procedure used for identifying active hosts on a network. This also extends to finding network addresses that do no map to a specific host.

Network Services: TAMUT group responsible for computer security, servers and network.

Information Technology: The name of the TAMUT department responsible for computers, networking and data management.

Vulnerability: a weakness or flaw in system security design, implementation, procedures or controls that can cause a violation of the system's security policy or a security breach if exploited by an attacker.

Wardriving: The act of searching for Wireless networks throughout a given area.

Procedures and Responsibilities

1. GUIDELINES AND PROCEDURES

1.1 A vulnerability assessment may include assessment(s) of any of the following information resources:

1.1.1 Network(s)

1.1.2 Operating System(s)

1.1.3 Application(s)

1.2 INFORMATION TECHNOLOGY will occasionally conduct network scans and network vulnerability scans on devices attached to the TAMUT network. This will give INFORMATION TECHNOLOGY personnel an overview of connected systems and their vulnerabilities.

1.3 Network scanning must only be conducted by the network services personnel or third parties who have been authorized by the IRM and ISO.

1.4 A vulnerability assessment will be conducted by DIR at least annually.

1.5 Under no circumstances must network scanning be conducted by unauthorized users.

1.6 Custodians of information resources found to be vulnerable in any way will be contacted concerning any identified risk(s). The custodian is responsible for ensuring that the identified risk(s) is mitigated in a timely manner.

1.7 From time to time, INFORMATION TECHNOLOGY will perform "wardriving" in order to find rogue wireless access points.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441

Contact Office

Information Security Officer
903-886-5425