29.01.99.K1.160 Security Monitoring Standard Administrative Procedure

Effective: April 1st, 2004
Revised: April 25th, 2013
Revised: March 28th, 2019
Next Scheduled Review: March 2024

Introduction

Security Monitoring is a method used at Texas A&M University-Kingsville (TAMUK) to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Data backup logs
- Vulnerability Scanning

Purpose

The purpose of this procedure is to ensure that information resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing, new security vulnerabilities, or new unforeseen threats to information resources. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include audit compliance, service level monitoring, performance measuring, limiting liability, and capacity planning. Security monitoring must have the capability to trigger alerts and send them to authorized iTech staff.

Audience

This procedure applies to individuals that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resource security.

Security Monitoring Policy

1. Automated tools provide real time notification of detected vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:
    a. Internet traffic
    b. Electronic mail traffic
    c. LAN traffic, protocols, and device inventory
    d. Operating System Vulnerabilities
2. The following files will be checked for signs of exploitation at a frequency determined by risk:
    a. Automatic intrusion detection system logs
    b. Firewall logs
    c. User account logs
    d. Network scanning logs
    e. System error logs
    f. Application logs
    g. Data backup logs
    h. Help desk trouble tickets
3. The following checks will be performed at least annually by assigned individuals:
    a. Password strength
    b. Expired or Unauthorized user accounts
    c. Unauthorized network devices
    d. Operating system and software licenses
4. Any security issues discovered will be reported to the Information Security Officer (ISO) for follow-up investigation.
5. The ISO is responsible for returning the information resource to an approved level of security control.

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
3. Computer Security Act of 1987
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
6. Foreign Corrupt Practices Act of 1977
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
13. Texas Government Code, Section 441

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404