Intrusion Detection

Introduction

Intrusion detection plays an important role in implementing and enforcing an organized security policy. As information systems grow in complexity, effective security systems must evolve. With the increase in the number of vulnerability points introduced by the use of distributed systems, some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

Purpose

Intrusion detection provides two important functions in protecting information resources:

- Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

Audience

The UTMB Intrusion Detection Practice Standard applies to all individuals who are responsible for the installation of new Information Resources (IR), the operations of existing IR, and individuals charged with IR Security.

Sensitive Digital Data Management

Sensitive Digital Data, as defined by UTS 165, includes social security numbers, Protected Health Information (PHI), Sensitive Research Data, digital Data associated with an individual and/or digital Data protected by law. Sensitive digital Data must be secured and protected while at rest (electronic storage on a hard drive, digital or optical media), mobile (laptop, PDA or flash drive) and in transit (via email or the Internet).

Privacy

Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of UTMB are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 1 TAC §§202 (Information Security Standards), Information Resource Standards and in the University of Texas System, UTS 165 - Information Resources Use and Security Policy.
Intrusion Detection, continued

Implications

- To allow UTMB to promptly respond to information attacks, perimeter security will include intrusion detection capabilities

- Whenever a systems administrator had good reason to believe that information resources have been compromised, the involved computer(s) must be immediately removed from the network.

- All security incidents must be properly and promptly reported.

Practice Standards

- Users reporting any anomalies in system performance and signs of wrongdoing should be directed to the Information Security Officer (ISO) at ext. 23838, the Computer Incident Response Team (CIRT) at ext. 23838, the IS Help Desk at ext. 25200, or to the UTMB Compliance Hotline at (800) 898-7679.

- All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the Incident Management Practice Standard.

- Operating system, user accounts, and application software audit logging processes must be enabled on all host and server systems as defined by UTMB Information Services.

- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.

- Audit logging of any firewalls and other network perimeter access control systems must be enabled.

- Audit logs from the perimeter access control systems must be monitored/reviewed daily by the system administrator.

- System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.

- Audit logs for servers and hosts on the internal, protected network shall be reviewed by the system administrator on a weekly basis. The system administrator will furnish any audit logs as requested by the ISO.
Intrusion Detection, continued

Practice Standards (cont)

- Network/host-based intrusion tools will be checked on a routine basis by the system administrator.
- All trouble reports received by system administrator personnel should be reviewed for symptoms that might indicate intrusive activity.

Disciplinary Actions

Violations of this policy may result in disciplinary action which may include termination for employees; a termination of employment relations in the case of contractors or consultants; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTMB IR access privileges, civil and/or criminal prosecution.

References

- UTMB Acceptable Use of Information Resources Policy
- UTMB Information Resources Security Policy
- UTMB IR Security Management Practice Standards Approval Process
- UTMB IR Security Glossary
- UT System UTS-165 Information Resource Security Program