Section	**IS Security Policies**	05/01/2005	-Effective
		12/10/2011	-Revised
Policy 2.00	**Intrusion Detection**	Information Services	-Author

Introduction

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security systems must evolve. With the proliferation of 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 TSSWCB Intrusion Detection Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resources Security.

Definitions

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Security Incident: In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Information Attack: An attempt to bypass the physical or information security measures and controls protecting an AIS. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Information Operations: Actions taken to affect adversary information and information systems while defending one’s own information and information systems.

Information Resources Manager (IRM): 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 state 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. If an agency does not designate an IRM, the title defaults to the agency’s Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

Definitions, continued

Information Security Officer (ISO): Responsible to the IRM for administering the information security functions within the agency. The ISO is the agency's internal and external point of contact for all information security matters.

Information Services (IS): The name of the agency department responsible for computers, networking and data management.

Host: A computer system that provides computer service for a number of users.

Server: A computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

Firewall: An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

Intrusion Detection Policy

- Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
- 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 system must be enabled.
- Audit logs from the perimeter access control systems must be monitored/reviewed regularly 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 must be reviewed on a regular basis.
- Host based intrusion tools will be checked on a routine.
- All trouble reports should be reviewed for symptoms that might indicate intrusive activity.
- All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the Incident Management Policy.
- Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the IS Help Desk.

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment 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 TSSWCB Information Resources access privileges, civil, and criminal prosecution.

Supporting Information	**This Security Policy is supported by the following Security Policy Standards**
Reference #	**Policy Standards detail**
1	IR Security controls must not be bypassed or disabled.
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.
14	The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.
17	All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the agency is protected from damage, monetary or otherwise. Owner and custodian departments shall have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.

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
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications