State of Vermont

Intrusion Detection and Prevention Policy

Date: 11-02-10
Approved by: Tom Pelham
Policy Number:

Table of Contents

1.0 Introduction 3
1.1 Authority 3
1.2 Purpose 3
1.3 Scope 4
2.0 Policy 4
2.1 Assessment 4
2.2 Implementation of Intrusion Prevention and Detection Capabilities 4
2.2.1 Personnel 4
2.2.2 Assets 4
2.2.3 Prevention Controls 5
2.3 Monitoring, Review & Detection 5
2.3.1 Security Audit Strategies 5
2.3.2 Alarms and Alerts 5
2.4 Incident Response 5
3.0 Policy Notification 5

1.0 Introduction

1.1 Authority

The Department of Information and Innovation (DII) was created in VSA 22 § 901 (1), “to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government.”

Managers, employees, records personnel, third party vendors and all others who connect to or handle State of Vermont networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff to ensure that the policy (1) meets legal requirements specific to the agency and its data and (2) can be effectively carried out by agency employees. If laws or regulations require more stringent requirements than stated in this policy, the internal policy created by the agency must explicitly state the more stringent requirements. Agencies shall not develop an internal policy with requirements lower than the minimum requirements listed in this policy.

1.2 Purpose

This policy is designed to protect the confidentiality, integrity and availability of data that is stored on State of Vermont devices and to protect the network from being infected by any hostile attack.

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.

Intrusion prevention is a preemptive approach to network security used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator.

1.3 Scope

The scope of this policy includes State of Vermont computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the state who use and administer such systems.

2.0 Policy

The State of Vermont is committed to intrusion detection as well as intrusion prevention capabilities as part of an overall, multi-layered information technology security design to prevent, monitor and identify system intrusion or misuse. The State shall develop a strategy for intrusion detection and prevention within the resource constraints for these activities. The goal is to deploy systems that provide robust and effective intrusion detection, raise awareness of actions that may cause intrusions, and prepare plans for effective response when intrusions occur. The policy includes the following elements:

2.1 Assessment

State IT department(s) shall develop and deploy intrusion detection and prevention guidelines, systems and procedures for assets identified as critical to the mission of the agency. Such assessments can be enhanced or developed using vulnerability tools such as discovery scanning or vulnerability scanning.

2.2 Implementation of Intrusion Prevention and Detection Capabilities

State IT department(s) shall evaluate, select and deploy intrusion detection and preventio capabilities compatible with the network infrastructure, policies and resources available for these activities. Intrusion detection and prevention capabilities shall address the following:

2.2.1 Personnel

Personnel shall be identified and properly trained to operate,interpret and maintain intrusion detection and prevention capabilities.

2.2.2 Assets

I Intrusion detection capabilities shall be in place to provide information related to unauthorized or irregular behavior on an agency computer, network or telecommunications system. In addition intrusion prevention capabilities shall be implemented to prevent unauthorized use, anomalies or attacks on computer, network or telecommunications systems. In addition, intrusion detection capabilities shall be in place to provide information related to unauthorized or irregular behavior on an agency computer, network or telecommunications system. Intrusion detection and prevention capabilities shall be implemented that encompass basic security procedures such as reviewing activity logs, and depending on the results of the assessment, may also include special purpose intrusion prevention and detection features such as those found on network-based, host-based, wireless, or network behavior analysis intrusion detection and prevention systems.

2.2.3 Prevention Controls

Intrusion prevention systems shall have controls set to respond to a perceived attack. Controls shall be set from the perspective of continuing service to meet business needs and objectives.

2.3 Monitoring, Review & Detection

Intrusion detection and prevention capabilities shall include guidelines for monitoring and analyzing system logs, notifications, warnings, alerts and audit logs. Agencies shall maintain and review information technology security audit logs and intrusion detection and prevention system alerts on a daily basis to determine if an intrusion or other type of security incident has occurred or has been prevented.

2.3.1 Security Audit Strategies

Agencies shall develop information security audit strategies and processes relevant to each system. The strategy shall include the definition of monitored assets, the types and techniques of intrusion detection systems or intrusion prevention systems to be used, where each intrusion detection system or intrusion prevention system will be deployed, resources responsible for monitoring, the types of attacks the intrusion detection systems or intrusion preventionsystems will be configured to detect or prevent and the methods that will be used for responses or alerts.

2.3.2 Alarms and Alerts

Thresholds for alarms and alerts shall be configured to identify possible intrusion detection or prevention events or violations of agency policy. Agency procedures shall address the disposition, retention and criticality of alerts.

2.4 Incident Response

State agencies will respond to security incidents in compliance with the Incident Handling Procedure found at: http://dii.vermont.gov/Policy_Central under the Security Section.

3.0 Policy Notification

Each state agency is responsible for ensuring that employees are aware of where policies are located on websites. Agencies are also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.