Audit Highlights

Highlights of Legislative Auditor report on the Security Over Selected State Agency Internet Sites, issued on February 28, 2006. Report # LA06-11.

Background

In 2004, the Legislative Auditor issued a report on Utilization and Security Over State Internet Sites. That was the first phase of our review over Internet security. That report focused on the Department of Information Technology (DoIT) and agencies whose networks were administered by DoIT employees. This audit is the second phase of our review and includes agencies which maintain their own networks. These include the State Gaming Control Board, the Department of Corrections, and the Public Employees' Benefits Program. Although these agencies maintain their own networks, standards created by the State should be followed, inasmuch as the standards apply to all but two Executive Branch state agencies.

The Nevada Information Technology Operations Committee (NITOC) is responsible for developing standards that apply to state agencies. NITOC is responsible for reviewing proposed standards from eight other working committees to ensure they are consistent with each other and generally acceptable to Nevada state agencies. The eight working committees are: IT Project Oversight, Security, Integration, Communications, IT Workforce, Enterprise Architecture, Electronic Records Management, and Technical Standards. As of July 2005, the NITOC Security working committee had produced 20 statewide Information Technology (IT) security standards.

Purpose of Audit

The purpose of this audit was to determine if controls are sufficient to ensure the security and integrity of selected state agencies' computer networks and information stored by those agencies. Our audit included a review of controls over Internet security at selected state agencies for fiscal year 2005.

Audit Recommendations

This audit report contains two recommendations to improve Internet security. The Department of Information Technology should create a standard for timeliness of patch installation. In addition, the Department should provide more ongoing assistance, training, and security assessments to state agencies regarding information security.

The Department accepted the two recommendations.

Status of Recommendations

The Department's 60-day plan for corrective action is due on May 23, 2006. In addition, the six-month report on the status of the audit recommendations is due November 27, 2006.

Security Over Selected State Agency Internet Sites

Results in Brief

More needs to be done to assist state agencies in securing their networks. The 2004 audit on Internet security and this audit indicate security weaknesses continue to exist in state agencies. For example, improvements are needed over devices that manage the flow of information throughout individual agencies' networks and the State. These devices require regular monitoring to ensure adequate security. Further improvements in controls are needed for users' computers including password settings, security updates, and antivirus software. In addition, state required security-related plans have not been created or are incomplete. Finally, controls to access sensitive computer equipment need more frequent monitoring.

These weaknesses, if left uncorrected, provide increased opportunities for malicious users to gain access to agency computers, or reduce the chances of effectively recovering from a disaster. The Department of Information Technology has the statutory authority and staff to provide assistance to state agencies. This assistance will be valuable to agencies in properly securing their information systems.

Principal Finding

The Department of Information Technology has statutory authority to assist and advise nearly every Executive Branch agency. However, more can be done. This assistance would help agencies overcome the security weaknesses we have noted in the last two audits. The recently formed Office of Information Security group within the Department will greatly aid efforts to provide proper security training and guidance to state agencies.

A router is a device that contains many rules to manage the flow of network traffic. The Gaming Control Board is the only agency in our review that maintains its own routers. For Gaming's three primary routers, we found 33 rules that did not conform to established benchmarks. The overall effect of not conforming to these benchmarks is to render a network less secure. We noted that the agency's staff took immediate action to reconfigure their routers.

A firewall is a device designed to prevent unauthorized access to a network. Gaming is the only agency in our review that maintains its own firewall. We found the policy for this firewall needs improvement. The policy did not address who is authorized to create or modify firewall settings. This policy change would ensure greater awareness of how the firewall should be administered, and reduce the risk of unauthorized changes.

Web servers are computers that contain websites. Gaming and the Department of Corrections maintain their own web servers. For both agencies combined, 41 changes were needed to ensure secure configuration. The changes included settings designed to prevent malicious users from intentionally overloading the servers and to prevent the servers from displaying sensitive information on the agencies' websites.

Computers need to periodically be updated with the latest security software updates, referred to as patches. Of Gaming's five network servers tested, two were missing critical patches. In addition, critical patches had not yet been installed on the Public Employees' Benefits Program's (PEBP) server. A statewide standard on how often critical patches should be installed would be helpful to state agencies.

Network servers are the computers used to run an agency's network. We found password settings on network servers that were not in accordance with state standards. These settings resulted in a less secure network. They included passwords of insufficient length, and passwords not changed frequently. In addition, passwords could be reused too frequently, and users were not locked out after three unsuccessful login attempts. We found these weaknesses at Gaming and Corrections.

Network servers contain accounts that are used to grant employees permission to use a network and its resources. We found that Gaming had three active user accounts belonging to former employees. This increases the risk of unauthorized access to the agency's network and its data.

Of the 50 desktop computers we tested for critical security patches at the three selected agencies, 35 needed updating. Some of these computers needed five or more critical patches.

Controls over physical access ensure that only appropriate users are allowed access to sensitive computer equipment. We discovered that Gaming's network room was accessible by 65 individuals. Once staff was made aware of this situation, they reduced this to eight employees who had a legitimate reason to access the network room.

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.us/audit (775) 684-6815.

Audit Division
Legislative Counsel Bureau