Executive Summary

Background

A web server is a computer running software to provide services to other computers and their users. There are two types of web servers: external and internal. The state's external web servers are vital in allowing the public access to state programs and services. For example, many state citizens register for hunting licenses and permits through the Automated Licensing System. The state's internal web servers perform a wide array of functions including allowing user access to non-public agency applications and data. Both internal and external web server application security weaknesses potentially allow a user to gain unauthorized access to alter web site programming or agency data. Additionally, web servers could potentially be put into production without state authorization. Without proper controls, unauthorized access and servers could allow access to any data for any services offered through state web servers.

Audit Objectives, Scope, and Methodology

Our audit focused on the security of the state's web servers and its applications. Due to state services being vital to both state internal users and the public, our audit objective was to determine the state has controls in place to mitigate unauthorized web server activity. Our scope included both state external and internal servers with access to the state network. We interviewed Department of Administration (DOA) staff responsible for state network enterprise policy-making and agency network administrators to determine agency control environments regarding web servers and applications. We also reviewed contracts and statements of work to determine areas of responsibility for web servers. We scanned address ranges and compared the results to known web server addresses to determine the potential for unauthorized web servers. Security over web servers and applications was tested through scanning web servers and state agency web sites with automated software tools.

Conclusion

Based on our work, we determined enterprise-wide policy is vague and does not fully define agency web server and application security. This has led to agencies applying differing, or, in some cases, no web server or application security. For example, agencies are not scanning their web applications for security weaknesses to update the applications as required by DOA enterprise policy. We also determined DOA is not performing standard security checks on external web servers before the servers are made available to the public as required by the Department's enterprise security policies. Although our scans for unauthorized external web servers did not identify any unauthorized servers, we determined the risk posed by these servers is substantial and DOA does not perform regular monitoring for these servers. DOA can strengthen controls over web server and application security by defining state web server and web server application security responsibilities in policy, notify agencies of these responsibilities, implement procedures to comply with enterprise web server and application policy and regularly monitor for unauthorized state external web servers.