LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors:
James Gillett
Angie Grove

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Kent Rice, Information Systems Audit Manager

DATE: June 2009

CC: Janet R. Kelly, Director, Department of Administration
Dick Clark, Chief Information Officer

RE: Follow-up IS Audit (09SP-19): State Web Server Security Audit (org. 08DP-02), Department of Administration

INTRODUCTION

We presented our information systems audit on *State Web Server Security* at the Department of Administration to the Legislative Audit Committee in January 2008. The report contains two recommendations relating to:

- Web server and web server application security, responsibilities and policy
- Rogue server detection

We requested and received information from Department of Administration (DOA) personnel regarding progress toward implementation of the report recommendations. This memorandum summarizes DOA's response and our follow-up work.

BACKGROUND

A web server is a computer running software (applications) to provide services to other computers and their users. Web server and web server application weaknesses potentially allow a user to gain unauthorized access to website 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.

FOLLOW-UP DISCUSSION

The following sections summarize the report recommendations, and the department's progress towards implementing the recommendations.

Web Server Security Responsibilities and Policy

At the time of our audit, management of web server and web server application security (both hereafter referred to as web server security) was the responsibility of individual agencies. Guidance for information technology on the state's network is issued by the Department of Administration's Information

Technology Services Division (ITSD) in the form of enterprise policy. Specific to web servers, the applicable policy was ENT-SEC-012, which required a specific ITSD bureau to perform a "standard security check" on each web server before it was allowed to be accessible to the public.

The audit determined ENT-SEC-012 did not define web server security responsibilities other than who was to perform a security check and when the checks were to occur. We also determined this policy had not been communicated to all agencies, which led to agencies applying differing or, in some cases, no web server security. Finally, we determined the ITSD bureau responsible for making the web server security checks was restructured in March 2007 and the policy was not changed to reflect the restructuring.

Recommendation #1

We Recommend the Department of Administration:

A. Define state web server and web server application security responsibilities in policy.

B. Notify all state agencies of their web server and web server applications security responsibilities.

C. Implement procedures to comply with Enterprise Security policy ENT-SEC-012.

A. Recommendation Status: **Being Implemented**

ITSD is in the process of releasing a new set of 19 information systems security enterprise policies based on a federally accepted information systems security framework. Two of the policies are now in effect, eight are under DOA legal review, with the last of the policies due to be released by December 2010. The existing enterprise policy regarding web servers (ENT-SEC-012), while recently changed to remove ITSD as responsible for web server security checks, still does not fully address web server security because it does not define all responsibilities. ITSD considers ENT-SEC-012 a legacy policy and has no plans to further update this specific policy; however, according to ITSD, the new enterprise policies will fully address security of information systems, including web server security, once all the new policies have been released.

B. Recommendation Status: **Being Implemented**

DOA is releasing information regarding the new enterprise policies through state information technology (IT) groups and email notifications to agency IT personnel and management. ITSD policy and security managers are also meeting directly with agency management. ITSD's modification of ENT-SEC-012, noted in the previous section, gave state agencies responsibility for web server security, and state agency IT management was notified of the change through IT groups and a statewide Chief Information Officer Advisory.

C. Recommendation Status: **Being Implemented**

At the time of the audit, ITSD did not have procedures in place allowing them to comply with ENT-SEC-012. Currently, they are in the process of developing and finalizing web server risk assessment policy and procedures in line with the new enterprise policies.

In summary, web server security is the responsibility of individual agencies; however, ITSD is responsible for implementing enterprise policy to provide guidance to agencies. While existing policy does not address all web server security responsibilities, ITSD represents the new information systems security enterprise policies will provide more guidance. As a result, there is an ongoing need for auditors to review and assess new policies as they are implemented.

Rogue Server Detection

Any web server created without authorization from the state is called a rogue server. Rogue servers can bypass all state defenses allowing unauthorized passing of sensitive data outside the state network, and potentially leaving these servers open to the same security weaknesses as any other web server and web server application. There is greater risk in the state's De-Militarized Zone (DMZ); the area of the state network where hardware and software prevent outside users from gaining direct access to servers inside the state network. Common business practice is to monitor the network, through scanning, to detect rogue servers. Our audit identified a potential for rogue web servers to operate inside the state's DMZ due to lack of scanning.

Recommendation #2

We recommend the Department of Administration scan the De-Militarized Zone for rogue servers on a regular basis.

Recommendation Status: **Implemented**

DOA has contracted a private security company to monitor servers attached to the network and network traffic; the contractor also has a list of servers authorized to operate in the DMZ. Rogue servers in the DMZ are detected by the contractor through analysis of network traffic. If detected, ITSD is notified and is responsible for follow-up on the notification. Although this method of detecting rogue servers does not directly address the recommendation, it does allow for detection and removal of rogue servers.

S:\Admin_Restricted\IS\Follow-up\09SP-19 webservr-Follow-up-memo.doc/ah