Performance Audit

Statewide UNIX Security Controls

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0563-15

Released:
December 2015

DTMB maintains and operates approximately 950 UNIX servers. Systems and data critical for the operation of State government reside on these servers. The DTMB Technical Services Division is responsible for their configuration, administration, and security. The Cloud Automation and Audit Compliance teams provide oversight and support for UNIX security.

Audit Objective			Conclusion
Objective #1: To assess the effectiveness of DTMB's efforts to implement security and access controls over the State's UNIX servers.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
DTMB did not establish and implement effective operating system security configuration controls for the State's UNIX server environment. We noted potentially vulnerable security configurations on 59 (94%) of 63 servers tested (Finding #1).	X		Agrees
DTMB should establish a strategy to ensure that only supported UNIX operating system versions are installed on servers containing the State's applications. Unsupported versions were operational on approximately 30 of the State's UNIX servers, some of which contained systems considered critical to State government operations (Finding #2).		X	Agrees
DTMB did not apply operating system patches in a timely manner for 90% of the servers tested. Patch management maintenance windows were not established for 559 (58%) of the State's UNIX servers (Finding #3).		X	Agrees
DTMB did not establish and implement effective access controls over the State's UNIX operating systems to help prevent or detect inappropriate access to data (Finding #4).		X	Agrees

Audit Objective			Conclusion
Objective #2: To assess the effectiveness of DTMB's efforts to establish an effective governance structure over the State's UNIX server environment.			Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not fully establish and implement effective procedures to detect and remediate security vulnerabilities. Forty-seven percent of servers tested did not have a vulnerability scan in over one month. When performed at our request, the average number of high risk exposures detected on a server was 77 and the greatest number was 420 (Finding #5).	X		Agrees
DTMB did not fully establish a segregation of duties over the administration of UNIX servers. The DTMB Agency Services Division had too much control over key processes, which increased the risk that controls designed to secure the State's information systems could be circumvented (Finding #6).		X	Agrees
DTMB did not maintain an accurate record of UNIX server information, which is necessary to maintain server security and to ensure the ready availability of information for critical business decisions (Finding #7).		X	Agrees

Observations Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB contracted with a third party vendor in 2009 for administration of certain UNIX servers at an annual cost of approximately $264,000. The contract required a transfer of knowledge to State employees. However, as of August 2015, the server administration functions were still performed by the vendor even though DTMB had 16 State employees capable of performing the functions (Observation #1).	Not applicable	Not applicable	Not applicable