Network and Cyber Security Audit

OAG

Office of the Auditor General

Presented by: Shelly Fanson
Keith Edwards

Preliminary Review and Scope

- Configuration, access, and monitoring for:
  - Firewalls
  - Switches
  - Routers
  - Wireless networks
- Cyber security
- State of Michigan (SOM) network
  - Next Generation Digital Infrastructure (NGDI) vs legacy
  - Roles and responsibilities

Report Summary

- Four objectives
- Fourteen findings
  - Five material conditions
  - Nine reportable conditions

Objective 1: Design and Administration of a Secure IT Network

To assess the sufficiency of DTMB's efforts to design and administer a secure IT network.

- Governance
- Network design and segmentation
- Inventory and End-of Life (EOL)
- Stability and availability

Finding 1: Configuration Management Controls

Fully establish and implement configuration management controls

- Adopt industry best practices
- Security configuration checklists and baseline configurations
- Configuration monitoring
- Change testing

Finding 2: Network Access Control

Implement a NAC solution.

- NMAP scan revealed approximately 87,000 IP addresses on the State's IT network.
- Initial comparison to the State's IT equipment inventories of record left more than 69,000 IP addresses unmatched.

Finding 3: Operating System Updates

Fully establish and implement an effective process for managing updates to the operating systems of network devices.

- 10 of 28 high or medium vendor- classified vulnerabilities that could potentially be exploited.
- No formal process for vulnerability review.
- The 3,126 devices reviewed run on a mix of 140 different OS versions.

Finding 4: Life Cycle Management

Fully establish and implement effective lifecycle management processes.

- 745 devices no longer supported by the vendor
- 190 devices running an OS no longer supported by the vendor
- 1,756 devices not covered by the EA roadmap
- EA roadmap contained insufficient or inaccurate information

Objective 2: Security and Access Controls

To assess the effectiveness of DTMB's security and access controls over the State's IT network.

- Network device configuration and access
- Firewall rules
- Wireless

Finding 8: Firewalls

Establish and implement effective controls for firewall management

- Periodically review firewall rulesets
- Review all changes to firewall rulesets
- Periodically test firewall rulesets
- Ruleset compliance with standards and best practices
- Document the review and approval of ruleset changes
- Monitor all firewalls

Finding 9: Network Device Configuration

Configure network device operating systems in accordance with best practices.

- 45 of 45 (100%) devices with deviations from best practices.
- Deviations per device ranged from 6 to 26 deviations.

Objective 3: Monitoring of Network Security

To assess the sufficiency of DTMB's efforts to monitor the security of the State's IT network.

- Risk assessments
- Network monitoring tools
- Vulnerability scans
- Penetration testing

Finding 11: Risk Management Practices

Risk management practices not fully established and implemented.

- Conduct risk assessment of the network.
- Identify and remediate vulnerabilities on network devices.
  - Authenticated scans not completed for 45 of 45 sampled devices.
  - Unauthenticated scans not completed for 38 of 45 sampled devices.
  - High and medium severity vulnerabilities not remediated timely.
  - 82 high and 167 medium severity vulnerabilities existed.
- Should further penetration testing efforts.

Objective 4: Cyber Security Awareness Programs

To assess the effectiveness of DTMB's cyber security awareness programs.

- Training participation rates
- Cyber security awareness survey
- Phishing campaign

Finding 14: Security Awareness Program

Security awareness program should continue.

- Assess the effectiveness of training.
- Ensure satisfactory participation rates.
  - An average of 68% of network users had completed the training.
- Phishing campaign results:

	Number of Employees	Percentage of Employees
Opened the e-mail	1,619	32%
Clicked the link within the e-mail	1,238	25%
Entered credentials	945	19%

Audit Report Impact

DTMB response

Media coverage

Legislative testimony

Questions?

Shelly Fanson: sfanson@audgen.michigan.gov

Keith Edwards: kedwards@audgen.michigan.gov