Network and Cyber Security Audit
Agenda

- Audit overview and scope
- Audit approach
- Key findings and takeaways
Preliminary Review and Scope

• State of Michigan (SOM) network
  • Next Generation Digital Infrastructure (NGDI) vs legacy
  • Roles and responsibilities

• Excluded extranets

• Configuration, access, and monitoring for:
  • Switches
  • Routers
  • Firewalls

• Cyber security
Report Summary

• Four objectives
• Fourteen findings
  • Five material conditions
  • Nine reportable conditions
Objective 1: Design and Administration of a Secure IT Network

Governance

Design & Segmentation

Inventory & End of Life (EOL)

Stability & Availability
Finding 1: Need to fully establish and implement configuration management controls *(Material)*.

Finding 2: NAC solution needed to help prevent unauthorized devices from connecting to the State’s network *(Material)*.

Finding 3: Improved process needed for managing updates to network device operating systems *(Material)*.

Finding 4: Network device lifecycle management processes need improvement *(Reportable)*.
Criteria:  NIST 800-128 Security-Focused Configuration Management

Methodology:
• Identified best practices used to configure network devices (Step 1.2)
• Compared security configuration checklists and baselines to industry best practices (Step 1.3)
• Reviewed configuration management processes (Step 1.4)
Fully establish and implement configuration management controls

- Adopt industry best practices
- Security configuration checklists and baseline configurations
- Configuration monitoring
- Change testing
Audit Approach: Network Access Control

Criteria: NIST 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations (IA-3, CM-8)

Methodology:

• Obtained network discovery reports (Step 1.15)
• Reviewed results and DTMB’s processes to match identified IP addresses to known IT equipment (Step 1.16)
Implement a NAC solution.

• NMAP scan revealed approximately 87,000 IP addresses on the State’s IT network.

• Initial comparison to IT equipment inventories of record left over 69,000 unmatched.
Criteria: NIST 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations (SI-2)

Methodology:

• Selected 4 network device OS versions for review (Step 1.9)
• Reviewed vendor security advisories for the selected OS versions (Step 1.10)
• Identified all vulnerabilities with severity of medium or higher (Step 1.10)
• Requested security impact analysis for all vulnerabilities that could potentially be exploited (Step 1.11)
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.
Audit Approach: Life Cycle Management


Methodology:
• Obtained an inventory of network devices (Step 1.5)
• Obtained vendor issued lifecycle statuses (Step 1.12)
• Reviewed the Enterprise Architecture (EA) roadmap (Step 1.13)
• Compared the EA roadmap and inventory to vendor lifecycle statuses (Step 1.14)
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

Network Device Configuration and Access

Firewall Rules

Wireless
Objective 2: Key Findings

Finding 8: Controls over firewalls need to be improved to ensure security of the network (*Material*).

Finding 9: Improvements in network device configurations needed (*Reportable*).
Audit Approach: Firewalls

Criteria:  NIST 800-41r1 Guidelines on Firewalls and Firewall Policy
           NIST 800-53r4 Security and Privacy Controls for Federal
           Information Systems and Organizations (CM-3)

Methodology:
• Obtained a population of firewall rulesets (Step 2.4)
• Selected a sample of 14 firewalls and reviewed the ruleset for compliance with best practices and standards (Step 2.5)
• Reviewed management practices for the sampled firewalls (Step 2.6)
• Selected a sample of 48 firewall rule changes for review (Step 2.7)
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
Audit Approach: Network Device Configuration

Criteria: NIST 800-128 Security-Focused Configuration Management Vendor Hardening Guides

Methodology:
• Obtain a population of supported network devices (Step 2.1)
• Selected a sample of 45 network devices for review for compliance with best practices and standards (Step 2.2)
Configure network device operating systems in accordance with best practices.

- 45 of 45 devices with deviations from best practices.
- Deviations per device ranged from 6 to 26 deviations.
Objective 3: Monitoring of Network Security

- Risk Assessments
- Network Monitoring Tools
- Vulnerability Scans
- Penetration Testing
Finding 11: Risk management practices not fully established and implemented (Material).
Audit Approach: Risk Management Practices

Criteria: NIST 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations (RA-3, RA-5, CA-8)

Methodology:

• Obtained and reviewed network risk assessments (Step 3.1)
• Conducted and reviewed vulnerability scan results for a sample of 45 network devices (Step 3.5)
• Reviewed results of penetration testing (Step 3.6)
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

Training Participation Rates

Cyber Security Awareness Survey

Phishing Campaign
Finding 14: Security awareness program should continue *(Reportable).*
Audit Approach: Security Awareness Program

Criteria: NIST 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations (AT-2)

Methodology:
- Reviewed participation rates of the cyber security awareness training program (Step 4.1)
- Conducted a survey to assess cyber security awareness for a sample of 12,500 network users (Step 4.2)
- Developed and performed a phishing campaign for a sample of 5,000 network users (Step 4.3)
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:

<table>
<thead>
<tr>
<th>Action</th>
<th>Number of Employees</th>
<th>Percentage of Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opened the e-mail</td>
<td>1,619</td>
<td>32%</td>
</tr>
<tr>
<td>Clicked the link within the e-mail</td>
<td>1,238</td>
<td>25%</td>
</tr>
<tr>
<td>Entered credentials</td>
<td>945</td>
<td>19%</td>
</tr>
</tbody>
</table>
Media coverage

Legislative testimony
Questions?

Keith Edwards: kedwards@audgen.michigan.gov

Jesse Soerries: jsoerries@audgen.michigan.gov