Policy Title: Vulnerability Scanning

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1405 (2014) Vulnerability Scanning

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Vulnerability scanning addresses the scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms which could pose threats to the University’s information system.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CONTACT(S)</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Information Technology – (757)823-2869</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STAKEHOLDER(S)</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Faculty &amp; Staff</td>
<td>2</td>
</tr>
<tr>
<td>Office of Information Technology</td>
<td>3</td>
</tr>
</tbody>
</table>

CONTACT(S)

Office of Information Technology – (757)823-2869

STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology
PURPOSE

This control is intended to establish the policy and procedures for vulnerability scanning utilized within the University’s information system.

REQUIREMENTS

NSU:

1. Scans for vulnerabilities in the information system and hosted applications at least once every 90-days for publicly facing systems and when new vulnerabilities potentially affecting the system/applications are identified and reported;

2. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
   a. Enumerating platforms, software flaws, and improper configurations;
   b. Formatting and making transparent, checklists and test procedures; and
   c. Measuring vulnerability impact.

3. Analyzes vulnerability scan reports and results from security control assessments;

4. Remediates legitimate vulnerabilities within 90 days in accordance with the University assessment of risk; and

5. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Supplemental Guidance: The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). The University considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

Control Enhancements for Sensitive Systems:

NSU:
1. Employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned;

2. Updates the list of information system vulnerabilities scanned at least once every 90 or when new vulnerabilities are identified and reported;

3. Employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked);

4. Attempts to discern what information about the information system is discoverable by adversaries;

5. Includes privileged access authorization to the University-identified information system components for selected vulnerability scanning activities to facilitate more thorough scanning;

6. Reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited; and

7. Scans for vulnerabilities in the sensitive information systems and hosted applications at least once every 90-days and when new vulnerabilities potentially affecting the system/applications are identified and reported.

VIOLATIONS

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

INTERPRETATION

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;
2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;

3. Post the policy on the appropriate SharePoint Site and/or Website; and

4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
- Revision History:
  - Supersedes (previous policy): OIT 62.8.1405 Vulnerability Scanning

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard