Effective Date: 6/28/2005
Revised Date:
Review Date:

North Sound Mental Health Administration

Section 4000 – Information Systems: Audit Vulnerability Scan

Authorizing Source:
Cancels:
See Also:
Responsible Staff: IS Specialist

Approved by: Executive Director
Motion #:

Date: 6/28/2005

POLICY #4003.00

SUBJECT: AUDIT VULNERABILITY SCAN

POLICY

At least annually, the IS/IT Department shall conduct audit vulnerability scans from both the inside and outside of the NSMHA network.

Internal Scans

When conducting internal scans, at a minimum, the following shall be done:

1. System user testing
    a. Randomly choose a current system user
    b. Make a copy of their profile
    c. Make attempts to access various network resources such as:
        i. Directories where the user does not have access
        ii. System tools that affect configuration of network resources
    d. Attempt to log on to resources that the user does not have access to log on to
    e. Attempt to bypass firewall settings
    f. Attempt to access potentially malicious files. Currently, most workstations are configured to not execute certain file types (e.g., .vbs, .js, etc.) but rather point to a warning documented located on the network.
2. Verify that various security and system logs are appropriately logging scan events.
3. Document any vulnerabilities found and propose solutions if necessary.
4. Rectify as applicable vulnerabilities found

This is by no means meant to be an exhaustive list of the internal scans that will be conducted. Rather it is to establish a minimum of what shall be done. Additional items will be scanned as technology and system resources change, and as new threats are discovered. These additional items scanned will be documented as a part of the report generated from the internal scans.

External Scans

When conducting external scans, at a minimum, the following shall be done:

1. Firewall testing
    a. Utilize various external resources to probe the firewalls to see what ports are open.
    b. Attempt to gain access to network resources via open ports

2. Test to ensure protection mechanisms are protecting NSMHA mailboxes by blocking potentially malicious attachments to email messages.
3. Test if able to bypass firewalls to gain access to internal network resources.
4. Verify that various security and system logs are appropriately logging scan events.
5. Document any vulnerabilities found and propose solutions if necessary.
6. Rectify as applicable vulnerabilities found

This is by no means meant to be an exhaustive list of the external scans that will be conducted. Rather it is to establish a minimum of what shall be done. Additional items will be scanned as technology and system resources change, and as new threats are discovered. These additional items scanned will be documented as a part of the report generated from the internal scans.

ATTACHMENTS

None