UTN Vulnerability Management Procedure

Revised with the recommendation of the UTN Advisory Council on 2/6/2016. The initial procedure was approved 2/20/2015 by the UETN Governing Board at the recommendation of the UTN Advisory Council and the UTN Technical Subcommittee. Implementation began May 28, 2015.

UTN conducts vulnerability scans of all systems connected to its private network that supports the delivery of healthcare systems and services for member sites. This procedure, focused on Level 5 vulnerabilities, is intended to encourage member sites to address vulnerabilities within a defined timeframe.

Definitions

Vulnerability: A weakness by which an intruder can easily gain control of a device, which can lead to the compromise of a site's entire network security. Any device that uses an IP address is vulnerable to being exploited. Vulnerabilities are rated on a scale of Level 1 – Level 5.
Level 5 vulnerability: The most severe vulnerability with the greatest risk of exploitation of a network. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.
Open vulnerability: An identified Level 5 vulnerability that has not been addressed.
Closed vulnerability: An identified Level 5 vulnerability that has been addressed by either 1) fixing the problem if feasible, or 2) through documentation if not.
Device: A computer, phone, tablet, printer or other machine that uses an IP address to connect into a network.

Communication Plan

1. Vulnerability scans occur weekly. Reporting and communication with site technical contacts are conducted through an issue tracking program.
2. Notifications of new Level 5s and a summary of all open Level 5 vulnerabilities are provided to site technical contacts weekly.
3. A monthly report will be emailed to site administration and technical contacts with an update on the following metrics for their site(s) and the network as a whole for Level 5 vulnerabilities: Total, # closed, % closed, # open, # sanctioned, # at threat of sanctions by the end of the month.
4. Site technical contacts are required to document when a Level 5 vulnerability cannot be corrected, such as one that required manufacturer intervention (a software upgrade, which they may/may not be willing to do) or replacement of capital equipment, which may be unrealistic. Once documented, these vulnerabilities will be removed from reporting for up to six month increments, at which time a review and documentation update is required.
5. UTN will provide documentation templates for optional use by site IT staff to assist with this process.
6. UTN will provide reports as requested by sites for use in security audits.

Sanctions

1. Sanctions will be imposed once a month following the last scan of the month.
2. Devices will be blocked when they have one or more Level 5 vulnerabilities open for 8 weeks or more as of the last scan of a month.
    a. The device will remain blocked until the vulnerabilities are addressed.
    b. Exceptions will be made for devices directly impacting patient care.
    c. Extensions may be requested via documentation.
3. If a site has one or more Level 5 vulnerabilities open for 16 weeks or more and has closed less than 90% of its Level 5 vulnerabilities as of the last scan of a month, it will be reported

to the UTN Advisory Council and UTN will engage the site in discussions regarding network membership.

Timeline

Procedure effective as of March 2, 2015
Revision effective as of February 4, 2016
Sanctions resume as of March 31, 2016.