Two updated guides provide latest NIST recommendations for system patches, malware avoidance

20 August 2013

The National Institute of Standards and Technology (NIST) has updated two of its series of computer security guides to help computer system managers protect their systems from hackers and malware. Vulnerabilities in software and firmware are the easiest ways to attack a system, and the two revised publications approach the problem by providing new guidance for software patching and warding off malware.

A common method to avoid attacks is to "patch" the vulnerabilities as soon as possible after the software company develops a piece of repair software—a patch—for the problem. Patch management is the process of identifying, acquiring, installing and verifying patches for products and systems.

The earlier guidance on patching, Creating a Patch and Vulnerability Management Program, was written when patching was a manual process. The revision, Guide to Enterprise Patch Management Technologies,* is designed for agencies that take advantage of automated patch management systems such as those based on NIST's Security Content Automation Protocol (SCAP).

Guide to Enterprise Patch Management Technologies explains the technology basics and covers metrics for assessing the technologies' effectiveness.

The second security document provides guidance to protect computer systems from malware—malicious code. Malware is the most common external threat to most systems and can cause widespread damage and disruption.

NIST's Guide to Malware Incident Prevention and Handling for Desktops and Laptops** was updated to help agencies protect against modern malware attacks that are more difficult to detect and eradicate than when the last version was published in 2005. The new guidance reflects the growing use of social engineering and the harvesting of social networking information for targeting attacks.

The new malware guide provides information on how to modernize an organization's malware incident prevention measures and suggests recommendations to enhance an organization's existing incident response capability to handle modern malware.

More information: *Guide to Enterprise Patch Management Technologies (NIST Special Publication 800-40, Revision 3) is available at: nvlpubs.nist.gov/nistpubs/Spec … NIST.SP.800-40r3.pdf

**Guide to Malware Incident Prevention and Handling for Desktops and Laptops (Special Publication 800-83 Revision 1) can be found at: nvlpubs.nist.gov/nistpubs/Spec … NIST.SP.800-83r1.pdf

Provided by National Institute of Standards and Technology

APA citation: Two updated guides provide latest NIST recommendations for system patches, malware avoidance (2013, August 20) retrieved 20 October 2019 from https://phys.org/news/2013-08-latest-nist-patches-malware.html