NIST updates guidance on network attacks and malware

July 26 2012

Detecting and stopping malicious attacks on computer networks is a central focus of computer security these days. The National Institute of Standards and Technology (NIST) is asking for comments on two updated guides on malicious computer attacks: one on preventing, detecting, and responding to attacks and one on preventing and mitigating the effects of malware, a potent tool in an attacker's arsenal.

The publications are being revised to reflect the changes in threats and incidents.

Malware, also known as malicious code, is a common tool that attackers use to breach computer networks today, causing damage and disruption, and often requiring extensive recovery efforts. "Malware threats in the past tended to spread quickly and were easy to discover," explains co-author Karen Scarfone, "but today's malware threats are stealthier, specifically designed to quietly, slowly spread, gathering information over extended time frames and eventually leading to loss of sensitive data and other problems."

The updated Guide to Intrusion Detection and Prevention Systems describes software that has become a necessary addition to the security infrastructure of many organizations.

Intrusion detection and prevention systems (IDPSs) record information about observed security-related events, notify security administrators of the events that should be analyzed further and produce reports for evaluation. Many IDPSs respond to and try to stop detected threats by using a variety of techniques.

The guidance describes the characteristics of IDPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring and maintaining them. The publication discusses four types of IDPS technologies: network-based, wireless, network behavior analysis and host-based.

"IDPS for wireless is an important type for all organizations to have because of the growth of mobile devices and employees' desire to use their own wireless device for work," says Scarfone.

While many agencies and companies are going mobile, it is still critical to protect desktops and laptops. The Guide to Malware Incident Prevention and Handling for Desktops and Laptops is a supplement to another draft document, Computer Security Incident Handling Guide (SP 800-61).* It gives background information on the major categories of malware that afflict desktop and laptop computers and provides practical guidance on how to prevent malware incidents and on what to do when a system is infected. The revised version of SP 800-61 is expected to be published later this summer.

Recommended measures include developing prevention plans based on the attacks that are most likely to be used now and in the near future, using defensive architecture methods to reduce the impact of malware incidents, and including malware incident prevention in employee awareness and training programs.

More information: The Guide to Intrusion Detection and Prevention Systems (Special Publication 800-94, Rev. 1) can be found at csrc.nist.gov/publications/dra … ft_sp800-94-rev1.pdf . Comments should be sent to 800-94comments@nist.gov by August 31.

The Guide to Malware Incident Prevention and Handling for Desktops and Laptops (Special Publications 800-83, Rev. 1) can be found at csrc.nist.gov/publications/dra … ft_sp800-83-rev1.pdf . Comments should be sent to 800-83comments@nist.gov by August 31.

The Computer Security Incident Handling Guide (SP 800-61, Rev. 2) is available at csrc.nist.gov/publications/Pub … s.html#SP-800-61-Rev .%202

Provided by National Institute of Standards and Technology

Citation: NIST updates guidance on network attacks and malware (2012, July 26) retrieved 26 April 2024 from https://phys.org/news/2012-07-nist-guidance-network-malware.html