How to Protect Your Web Server from Attacks

October 11 2007

The National Institute of Standards and Technology has released a new publication that provides detailed tips on how to make web servers more resistant to potential attacks. Called “Guidelines on Securing Public Web Servers,” the publication covers some of the latest threats to web security, while reflecting general changes in web technology that have taken place since the first version of the guide was published 5 years ago.

Web servers are the software programs that make information available over the Internet. They are often the most frequently targeted hosts on a computer network.

Attackers gaining unauthorized access to the server may be able to change information on the site (e.g., defacing a web page), access sensitive personal information, or install malicious software to launch further attacks. Recently emerging threats include “pharming,” in which people attempting to visit a web site are redirected surreptitiously to a malicious site.

How does one thwart these attacks? The guide advocates taking basic steps such as keeping up-to-date on patches (fixes and updates) for web server software and the underlying operating system. Also, the guide recommends configuring the software in as secure a fashion as possible, for example by disabling unnecessary software services and applications, which may themselves have security holes that can provide openings for attacks.

Another key recommendation, especially for large-scale operations, is to consider the proper human-resource requirements for deploying and operating a secure web server, by staffing the appropriate complement of IT experts (such as system and network administrators) all doing their jobs to establish and promote security.

The guide advocates “defense in depth”—installing safeguards at various points of entry into the server, from the router that handles all incoming data traffic to the specific machines that house the server software. In addition, the guide recommends, organizations should monitor log files, create procedures for recovering from attacks, and regularly test the security of their systems.

The guide is designed for federal departments and agencies, but may be applicable to any web server to which the outside world has access. The guide is available free of charge at csrc.nist.gov/publications/nis … -ver2/SP800-44v2.pdf .

Source: NIST