The Hanover Insurance Group™

Hanover Risk Solutions

Key Guidelines for Securing Public Web Servers

Attacks on Web sites have shown that the computers that support Web sites are vulnerable to attacks, which can range from minor nuisances to significant interruptions of service. This report discusses the most commonly employed methods for protecting Web servers and provides key, practical guidance on steps that organizations can take to reduce the threat of attacks.

The World Wide Web (WWW) is a system for exchanging information over the Internet. Many organizations in industry, government, and academia use the Internet to publish and exchange information, serve their customers and the public, and conduct electronic transactions.

At the most basic level, the WWW can be divided into two principal components: Web servers and Web browsers. The Web server is the essential system component for providing functionality. The Web browser is the corresponding software application on the user's computer. It accesses the information that is stored on Web servers and displays it for the user.

While both Web servers and Web browsers are vulnerable to malicious intruders who can break into public Web sites, destroy or change information, and disrupt operations, the Web server is the most targeted and attacked host on most organizations' network. As a result, it is essential to secure Web servers and the network infrastructure that supports them.

This report provides a summary of Special Publication 800-44, Guidelines on Securing Public Web Servers, published by the Computer Security Division, Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). The ITL publication provides information on securing, installing, and configuring the operating system; securing, installing, and configuring Web server software; deploying appropriate network protection mechanisms, such as firewalls, routers, switches, and intrusion detection systems (IDSs); maintaining the secure configuration through application of appropriate patches and upgrades, security testing, monitoring of logs, and backups of data and operating system; and using, publicizing, and protecting information and data in a careful and systematic manner.

Threats to Web Servers

Because Web servers are one of the few system components on a target network that typically communicates with third parties, they are frequently the targets of malicious attacks by intruders. Intruders can easily launch automated attacks against thousands of systems simultaneously to identify the relatively few vulnerable systems. New

continued ▶

attacks can be set up and launched quickly from remote locations, foiling attempts by organizations to develop effective countermeasures. Once Web servers have been compromised, the organization's other network resources are at greater risk.

The specific security threats to Web servers generally fall into one of the following categories:

- Malicious entities may exploit software bugs in the Web server, underlying operating system, or active content to gain unauthorized access to the Web server. Examples of unauthorized access are gaining access to files or folders that were not meant to be publicly accessible or executing privileged commands and/or installing software on the Web server.
- Denial of service (DoS) attacks may be directed to the Web server denying valid users an ability to use the Web server for the duration of the attack.
- Sensitive information on the Web server may be distributed to unauthorized individuals.
- Sensitive information that is not encrypted when transmitted between the Web server and the browser may be intercepted.
- Information on the Web server may be changed for malicious purposes. Web site defacement is a commonly reported example of this threat.
- Malicious entities may gain unauthorized access to resources elsewhere in the organization's computer network via a successful attack on the Web server.
- Malicious entities may attack external organizations from a compromised Web server, concealing their actual identities, and perhaps making the organization from which the attack was launched liable for damages.
- The server may be used as a distribution point for illegally copied software, attack tools, or pornography, perhaps making the organization liable for damages.

For detailed information on computer incidents (i.e., types of attacks and security measures to prevent attacks), see Crime Prevention Report CP-85-12, *Preventing Computer Incidents*.

Key Security Guidelines

Intrusions can be very costly to the organization in terms of money, time, and damage to reputation. The confidentiality and/or integrity of the stored data can be jeopardized. Availability may also be affected, making the information on the organization's Web site effectively unobtainable. In addition, a compromised Web server could be used to distribute illegally copied software, attack tools, and pornography or as a base from which to attack other networks, possibly exposing the organization to legal liability.

Organizations need a security plan and a policy for implementing the plan, monitoring its effectiveness, and updating it. All those involved with or affected by the information processing systems have a role in protecting the security and the privacy of information assets. Security plans should include an overview of the security requirements of the system, the controls needed to meet those requirements, and the responsibilities of all individuals who access the system. With this basic planning as the foundation for secure systems, organizations should apply the following recommendations to improve the security of their Web servers (for more detailed information on these key guidelines, go to http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf):

1. Plan carefully and address the security aspects of deployment of Web servers.

Careful planning is essential before the installation, configuration, and deployment of Web servers. It is more difficult to address security issues once deployment and implementation have been completed. A detailed and well-designed deployment plan facilitates the organization's decisions about tradeoffs between usability, performance, and risks. A deployment plan makes it possible to maintain secure configurations and to identify security vulnerabilities.

The deployment plan should address:

- The purpose of the Web server, the information to be stored on or processed through the server, and the security requirements of the information and of related systems, networks, and services.
- The human resource requirements for the deployment and operational phases of Web servers and their supporting infrastructures, including the types of personnel, their skills and training, and levels of effort required.

2. Implement appropriate security management practices and controls to maintain and operate a secure Web site.

Appropriate management practices are critical to operating and maintaining secure Web servers. Organizations should identify their information system assets and determine the policies, standards, procedures, and guidelines that are needed to support the confidentiality, integrity, and availability of information system resources. All management controls that are required to protect information system assets should be developed, documented, and implemented. NIST recommends that organizations apply the following practices to ensure the security of Web servers and their supporting network infrastructure:

- Organizational-wide information system security policy.
- Configuration/change control and management.
- Risk assessment and management.
- Standardized software configurations that satisfy the information system security policy.
- Security awareness and training.
- Contingency planning, continuity of operations, and disaster recovery.
- Certification and accreditation.

3. Deploy, configure, and manage Web server operating systems to meet the security requirements of the organization.

The first step in securing a Web server is securing the underlying operating system. Most commonly available Web servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems supporting the Web servers are configured appropriately.

The default hardware and software configurations of Web servers may be set by vendors to emphasize features, functions, and ease of use, rather than the security of the system. Since each organization's security requirements are very different, Web administrators should configure new servers to reflect their organization's security requirements. When these requirements change, the Web servers should be reconfigured.

The steps needed to secure the operating system include:

- Patch and upgrade the operating system, as necessary.
- Remove or disable unnecessary services and applications.

- Configure operating system user authentication.
- Configure resource controls.
- Test the security of the operating system.

4. Web server applications should be deployed, configured, and managed to meet the security requirements of the organization.

In many respects, the requirements for secure installation and configuration of Web server applications are the same as for the operating systems. First and foremost, only the minimal and necessary portion of Web server services should be installed. If vulnerabilities are identified, they should be eliminated through patches or upgrades. Unnecessary applications, services, and scripts should be removed immediately after the installation process has been completed. The steps that should be taken to secure the Web server application include:

- Patch and upgrade the Web server application, as necessary.
- Remove or disable unnecessary services, applications, and sample content.
- Configure Web server user authentication.
- Configure Web server resource controls.
- Test the security of the Web server application and Web content.

5. Ensure that only appropriate content is published on the Web site and that the content is adequately protected from unauthorized alteration.

Organizations should develop a Web publishing process or a policy that determines what information may be published openly, what information may be published with restricted access, and what information should not be published in any publicly accessible repository. Web sites are vulnerable to individuals who mine an organization's Web site in search of valuable information. In general, the following kinds of information should be carefully examined and reviewed before publication on a public Web site:

- Classified or proprietary information.
- Information on the composition or preparation of hazardous materials or toxins.
- Sensitive information relating to homeland security.
- An organization's detailed physical and information security safeguards.
- Details about an organization's network and information system infrastructure (e.g., address ranges, naming conventions, and access numbers).
- Information that specifies or implies physical security vulnerabilities.
- Detailed plans, maps, diagrams, aerial photographs, and architectural drawings of organizational buildings, properties, or installations.

6. Take appropriate steps to protect Web content from unauthorized access or modification.

Organizations should control the information that is made available on public Web sites through their publishing processes or policies. Websites should be protected to assure that the information is not modified without authorization. Users rely on the integrity of the information made available to them. Because the information on public Web sites is easily accessible, it is more vulnerable to tampering and change than the information that is made available by the organization in other ways. Public Web content must be protected through the appropriate configuration of Web server resource controls. Some of the

resource control practices that should be applied include:

- Install or enable only necessary services.
- Install Web content on a dedicated hard drive or logical partition.
- Limit uploads to directories that are not readable by the Web server.
- Define a single directory for all external scripts or programs executed as part of Web content.
- Disable the use of hard or symbolic links.
- Define a complete Web content access matrix that identifies which folders and files within the Web server document directory are restricted and which are accessible (and by whom).
- Disable directory listings.
- Use user authentication, digital signatures, and other cryptographic mechanisms as appropriate.
- Use host-based intrusion detection systems and/or file integrity checkers to detect intrusions and verify Web content.

7. Active content should be used only after careful consideration of the benefits to be gained and the associated risks.

Interactive elements, supported by technologies, such as ActiveX, Java, VBScript, and JavaScript, enable users to interact with Web sites in new ways. No longer confined just to accessing text-based documents, users can carry out a wide range of applications. These interactive elements introduce new Web-related vulnerabilities since they involve moving code from a Web server to a client application for execution.

Users are at risk because active content can take actions on the user's computer without the permission or knowledge of the user. Content generation technologies on the Web server pose a similar risk because, when accepting input from users, they may be induced to take actions that could harm the server. One such risk is accepting large amounts of information that can overflow

buffers and be used to execute commands or gain unauthorized access to the Web server. All content must be protected, and close attention should be given to proper programming of browsers and servers. The different active content technologies have different vulnerabilities associated with them, and all must be carefully considered to balance benefits and risks.

8. Authentication and cryptographic technologies should be used appropriately to protect certain types of sensitive data.

Organizations should examine all of the information available on their public Web servers and determine their requirements to protect the integrity and confidentiality of that information. Web servers can support a range of authentication and encryption technologies, which can be used to identify and authenticate users with different privileges for accessing information. Using appropriate user authentication techniques, organizations can selectively restrict access to specific information. Otherwise, all information on a public Web server could be accessed by anyone with access to the server. Certain user authentication processes protect the user as well by enabling the user to verify the server being accessed is the "authentic" Web server and not a counterfeit version operated by a malicious entity.

Technologies based on cryptographic functions can provide an encrypted channel

between a Web browser client and a Web server that supports encryption. Web servers may be configured to use different cryptographic algorithms, providing varying levels of security and performance.

9. Use the network infrastructure to help protect public Web servers.

The network infrastructure that supports the Web server plays a significant role in the security of the Web server. With careful configuration and deployment, the network infrastructure can be used to protect the public Web server. Network design is influenced by factors such as cost, performance, and reliability, as well as by security. But network design alone cannot protect a Web server. The frequency, sophistication, and variety of Web attacks carried out today reinforce the need for layered and diverse defense mechanisms. Some of these defense-in-depth mechanisms include selection of a relatively safe network on which the public Web server will be located and configuration of the network to support and protect the Web server.

10. An ongoing process must be used to maintain the continued security of public Web servers.

Maintaining a secure Web server requires constant effort, resources, and vigilance. After a Web server has been deployed, Web administrators must monitor it on a daily basis to assure the continuing level of security. The following steps are essential to maintaining the security of a Web server:

- Configuring, protecting, and analyzing log files.
- Backing up critical information frequently.
- Maintaining a protected authoritative copy of the organization's Web content.
- Establishing and following procedures for recovering from compromise.
- Testing and applying patches in a timely manner.
- Testing security periodically.

Summary

Organizations and users benefit when access to public Web servers is safe and convenient and when the organization's electronic information resources are secure, reliable, and available. As is the case with all other aspects of remote access to organizational resources, the use of public Web servers entails risks, as well as benefits. These risks and benefits must be managed through careful planning and through implementation of guidelines for secure operation of public Web servers.

References

1. Information Technology Laboratory. Guidelines for Securing Public Web Servers. Special Publication 800-44. Gaithersburg, MD: National Institute of Standards and Technology, 2002. <http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf>

To learn more about Hanover Risk Solutions, visit hanoverrisksolutions.com

The Hanover Insurance Group™

The Hanover Insurance Company
440 Lincoln Street, Worcester, MA 01653

hanover.com
The Agency Place (TAP)—https://tap.hanover.com

171-0982 (3/14) LC 11-125