Securing a Web Site

Erik Evans

March 2006

Table of Contents

Listings

Introduction

Web servers are frequently attacked more than any other host on an organization's network. In this paper, I will review the current challenges businesses face when hosting a public web site. I will address the various risks that are associated with web servers as well as the most effective methods of mitigating those risks through the design, implementation, and administration of public web sites.

Issues That Increase Vulnerabilities

There are many levels to web site security; therefore, in order to reduce vulnerabilities, a public Web server must be properly secured at each level.

The first level that a Web server must be secured at is at the physical level. Because the Web server is susceptible to many types of attacks, both logical and physical, it is imperative that a physically secure location is setup to house the server(s). This area should be locked and access must be limited to only the individuals that have a legitimate reason to have physical access to the Web server (Kessler 2000). The area should have appropriate environmental controls so that the necessary humidity and temperature are maintained. In addition to this, the server should have a backup power source.

The next level at which the Web server must be secured is at the network level. If there are inadequate defense mechanisms to aid in preventing attacks at the network level, the whole web site could be brought down due to an attack such as a DoS attack.

The third level at which the web site needs to be secured is at the operating system level. If there are unnecessary services and/or programs running on the server, this can create vulnerabilities within the Web server. These vulnerabilities would give way for additional avenues of attack that could lead to the eventual compromise of the Web server itself.

The fourth level of concern for Web server security concerns the installing and configuring of the Web server applications. If there are vulnerabilities within the Web server software an attacker could compromise the security of the server as well as other hosts on the organization's network. This could be done by defacing the Web site, gaining unauthorized access to resources on the server or on other servers within the network, executing unauthorized commands or programs on the server, or using the server as a launching pad to attack other networks.

The fifth level deals with the security of the Web site itself, if there are poorly written applications or scripts on the Web site, this could allow attackers to compromise the security of the Web server as well as other hosts on the network. If not properly secured, vulnerabilities such as cross-site scripting or SQL injection could be created.

The last level of Web server security is in the continual act of administering the Web server once it is in place. It is important to ensure that a public Web site does not contain sensitive or confidential information that would put the company's assets at risk. Examples of this would be a Web site that contains information about the administrative accounts for the network or detailed information about the network infrastructure. In addition to this, it is necessary to have policies and procedures in place for supporting the Web server as patches/updates are released to address vulnerabilities.

Planning and Preparation

Before hosting a public Web site, take steps to make certain that the organization has an adequate security policy in place. The security policy should address the following areas:

- Step 1: Securing, installing, and configuring the underlying operating system of the Web server.
- Step 2: Securing, installing, and configuring Web server software.
- Step 3: Employing appropriate network protection mechanisms (e.g., firewall, packet filtering router, and proxy)
- Step 4: Maintaining the secure configuration through application of appropriate patches and upgrades, security testing, monitoring or logs and backups of data and operating system.
- Step 5: Using, publicizing, and protecting information and data in a careful systematic manner.
- Step 6: Employing secure administration and maintenance processes (including server/application updating and log reviews).
- Step 7: Conducting initial and periodic vulnerability scans of each public Web server and supporting network infrastructure (e.g., firewalls, routers).

LISTING 1 – (Tracy, Jansen, & McLamon 2002)

In order to make certain that the environment is secure, security must be thoroughly involved throughout each part of the Web server deployment (Prescatore 2003). It is much more difficult to address security requirements after a project is in progress, so it is essential that detailed planning is done at the beginning of setting up a Web site (Tracy, Jansen, & McLamon 2002). When planning to deploy a Web site, consider the following steps:

- Identify the purpose(s) of the Web server.
  - What information categories will be stored on the Web server?
  - What information categories will be processed on or transmitted through the web server?
  - What are the security requirements for this information?
  - Is any information retrieved from or stored on another host (e.g., backend database, mail server, proxy servers)?
  - What other service(s) does the Web server provide? (a Web server should run only on a dedicated host)
  - What are the security requirements for these additional services?
- Identify the network services that will be provided on the Web server, such as those supplied through the following protocols:
  - HTTP
  - HTTPS
  - Secure Hypertext Transfer Protocol (S-HTTP)
  - Remote Authentication Dial-In User Service (RADIUS) Protocol

- Open Database Connectivity (ODBC) Protocol
  - Network File System (NFS) Protocol
  - Common Internet File System (CIFS)
  - Internet Caching Protocol (ICP)
- Identify any network service software, both client and server, to be installed on the Web server and any other support servers.
- Identify the users or categories of users of the Web server and any support hosts.
- Decide if and how users will be authenticated and how authentication data will be protected.
- Determine how appropriate access to information resources will be enforced.

LISTING 2 – (Tracy, Jansen, & McLamon 2002)

Securing the Network Infrastructure of the Web Server

In most configurations, the network infrastructure will be the first line of defense between the Internet and a public Web server (Tracy, Jansen, & McLamon 2002). In this section, I will look at those network components that can support and protect Web servers to increase their overall security. However, it is important to keep in mind that network design alone cannot protect a Web server. With such a variety of Web attacks in our world today, Web security must have layered and diverse defense mechanisms (defense in depth) (Tracy, Jansen, & McLamon 2002).

Before I get too far in to the security of the network infrastructure, it is important to discuss whether an organization may wish to outsource the hosting of their Web site to another company. Many organizations choose to outsource the hosting of their Web server to a third party. The advantages of outsourcing from a security standpoint are as follows:

- DoS attacks aimed at the Web server have no effect on the organization’s production network.
- Compromise of the Web server does not directly threaten the internal production network.
- Outsourcer may have greater knowledge in securing and protecting Web servers.
- The network can be optimized solely for the support and protection of Web servers.

LISTING 3 – (Tracy, Jansen, & McLamon 2002)

The disadvantages of outsourcing from a security standpoint are as follows:

- Requires trusting a third party with Web server content.
- It is difficult to remotely administer the Web server or remotely update Web server content.
- Less control can be provided over the security of the Web server.
- Web server may be affected by attacks aimed at other Web server hosted by outsourcer on the same network.

LISTING 4 – (Tracy, Jansen, & McLamon 2002)

If the organization is smaller, outsourcing is a good option because it cuts down on the cost of the Web server staff that would have to be on hand to support the Web server(s) (Tracy, Jansen, & McLamon 2002). However, for larger organizations and organizations that wish to maintain tight control over the security of their Web server, it may be a better option to host the Web site internally (Tracy, Jansen, & McLamon 2002).

When hosting a Web site on an organization's network, a Demilitarized Zone is a good solution for where to place the Web server(s) (Kessler 2000). A Demilitarized Zone (DMZ) is a host or network segment inserted as a "neutral zone" between an organization's private network and the Internet (Tracy, Jansen, & McLamon 2002). It prevents external users of the Web server from obtaining access directly to an organization's internal network (intranet). A DMZ offers a way to keep a Web server out of the internal network while not exposing it directly to the internet.

Although there are multiple ways to create a DMZ, it is recommended to place a firewall between the border router and the DMZ and then another firewall between the DMZ and the internal network. Since the firewalls can have a more complex security rule set, superior safety is provided to the servers within the DMZ (Tracy, Jansen, & McLamon 2002). This configuration allows the analyses of incoming and outgoing HTTP traffic and can detect and protect against application layer attacks designed to compromise the security of the Web server (Tracy, Jansen, & McLamon 2002). The advantages of a DMZ from a security standpoint are as follows:

- Web server may be better protected and network traffic to and from the Web server can be monitored.
- Compromise of the Web server does not directly threaten the internal production network.
- Greater control can be provided over the security of the Web server since traffic to and from the Web server can be controlled.
- DMZ network configuration can be optimized to support and protect the Web server(s).

LISTING 5 – (Tracy, Jansen, & McLamon 2002)

The disadvantages of a DMZ from a security standpoint are as follows:

- DoS attacks aimed at the Web server may have an effect on the internal network.
- Depending on the traffic allowed to and from the DMZ and internal network, it is possible that the Web server can be used to attack or compromise hosts on the internal network.

LISTING 6 – (Tracy, Jansen, & McLamon 2002)

A DMZ is a necessity for organizations that support their own Web servers. However, it should only be considered secure when employed in conjunction with the other steps discussed in this document.

After the Web server is in place on the network, the components that make up the network infrastructure must be configured so that they can protect and support the Web server. The components of network infrastructure that support Web server security include firewalls, intrusion detection systems, intrusion prevention systems, network switches, and routers. Each component is important and has a unique role in protecting the Web server through defense in depth.

To protect a Web server using a firewall, ensure that it is capable of and configured to do the following:

- Control all traffic between the Internet and the Web server
- Block all inbound traffic to the Web server except TCP ports 80 (HTTP) and/or 443 (HTTPS)

- Block all inbound traffic with an internal IP address (to prevent IP spoofing attacks)
- Block client connections from the Web server to the Internet and the organization's internal network (this will reduce the impact of certain worms such as Code Red)
- Block (in conjunction with the intrusion detection and prevention system) IP addresses or subnets that the IDS/IPS reports are attacking the organizational network
- Notify the network administrator or appropriate security personnel of suspicious activity through an appropriate means (e.g., page, e-mail and network trap)
- Provide content filtering
- Protect against denial of service attacks
- Detect malformed or known attack URL requests
- Log critical events including the following details:
    - Time and date
    - Interface IP address
    - Vendor-specific event name
    - Standard attack event (if one exists)
    - Source and destination IP address
    - Source and destination port numbers
    - Network protocol used by attack
- Be patched to the latest or most secure level (firewall application and underlying operating system)

LISTING 7 – (Tracy, Jansen, & McLamon 2002)

A firewall is a critical first line of defense, but Web server applications are still susceptible to attack through TCP port 80 even with the configuration I just mentioned (Tracy, Jansen, & McLamon 2002). With this in mind, an organization must practice defense in depth in order to secure the Web server as good as possible.

An IDS is an application that monitors system and network resources and activities. Using the information gathered from these sources, the IDS notifies the network administrator and/or appropriate security personnel when it identifies a possible intrusion or penetration attempt (Tracy, Jansen, & McLamon 2002). An IPS is a hardware or software device that monitors system and network resources, this device has the ability to both detect and prevent known attacks (Secure Computing Corporate, 2003). The two principal types of IDS/IPS are host-based and network-based. A combination of these two technologies offers the most security for an organizations network and/or Web server.

Host-based IDSs/IPSs are useful when most of the network traffic to and from the Web server is encrypted because the functionality and capability of network-based IDSs/IPSs is severely limited when network traffic is encrypted (Tracy, Jansen, & McLamon 2002). Something to consider when deploying a host-based IDS/IPS system is a file integrity checker. This allows an administrator to monitor changes to critical files, such as Web content. Often, host-based IDS/IPS systems include the capability of a file integrity checker. When using a file integrity checker, be sure to have a process in place to update the checksum database anytime the system is updated or patched, this will help to avoid false alarms (Tracy, Jansen, & McLamon 2002). However, if the IDS/IPS does detect unauthorized system file modifications, an investigation should be opened according to the organization's incident response process.

Unlike Host-based IDSs/IPSs, network-based IDSs/IPSs can monitor multiple hosts and even multiple network segments simultaneously. They can usually detect and prevent more network-based attacks and can more easily provide a comprehensive picture of the current attacks against a network (Tracy, Jansen, & McLamon 2002). To successfully protect a Web server using an IDS and IPS, ensure that it is capable of and configured to accomplish the following tasks:

- Monitor network traffic before any firewall or filter router (network-based)
- Monitor network traffic to and from the Web server
- Monitor changes to critical files on the Web server (host-based or file-integrity checker)
- Monitor the system resources available on the Web server (host-based)
- Block IP addresses or subnets that are attacking the organizational network
- Prevent and notify the network or Web administrator of known attacks through appropriate means
- Detect port scanning probes
- Detect DoS attacks
- Detect malformed URL requests
- Log events including the following details:
    - Time and date
    - Interface IP address
    - Vendor-specific event name

    - Standard attack event (if one exists)
    - Source and destination IP address
    - Source and destination port numbers
    - Network protocol used by attack
- Be updated with new attack signatures frequently (at least on a weekly basis)

LISTING 8 – (Tracy, Jansen, & McLamon 2002)

Securing the Operating System

The next step to securing a Web server is to secure the operating system. Default hardware and software configurations are typically set by vendors to emphasize features, ease of use, and performance while sacrificing some security (Tracy, Jansen, & McLamon 2002). New servers must be configured to comply with the organization's security requirements. As a general rule, when configuring the operating system, disable, or even better, remove all services and applications that are not needed by the Web server (Tracy, Jansen, & McLamon 2002). It is better to remove services rather than disable them because some attacks attempt to alter settings within the operating system and would be able to activate a disabled service (Tracy, Jansen, & McLamon 2002). This threat is mitigated when the service does not exist on a given host. If possible, install the minimal operating system configuration that is required for the Web server application because many uninstall programs do not completely remove all of the elements of a service (Tracy, Jansen, & McLamon 2002).

Next, all necessary patches and updates that have been released to address known vulnerabilities within the OS should be tested and then applied. In addition to this, be sure that the organization has a process for identifying known vulnerabilities and applying patches and addressing them as necessary in the future.

The third step to securing the OS is to ensure appropriate user authentication is in place by taking the following steps:

- Remove or disable all unneeded default accounts and groups.
- Disable accounts that are not interactive. Disable accounts that need to exist but do not require an interactive login.
- Create the user groups. Assign user to the appropriate groups, then assign rights to the groups.
- Create the user accounts. Identify who will be authorized to use each computer and its services. Create only the necessary accounts.
- Check the organization's password policy and make sure that all local accounts conform to the policy.
- Configure the server to deny login after a small number of failed attempts.
- If remote administration is not going to be implemented, disable the ability for the administrator or any other account to log in from the network.
- Periodically review the list of user accounts to ensure that all existing user accounts are needed.

LISTING 9 – (Tracy, Jansen, & McLamon 2002)

The fourth step should be to set access control lists to system resources following the principle of least privilege. Authorized system administrators should be the only users that are able to execute most system administration tools, this can prevent users from making changes to the system that would reduce security and restrict an intruder's ability to use the tools in the event of an attack (Tracy, Jansen, & McLamon 2002).

The last step is to perform periodic security testing of the operating system. This is a good way to identify vulnerabilities as well as verify that the existing security measures are effectively protecting your assets (Tracy, Jansen, & McLamon 2002). In order to do this, a combination of vulnerability scanning and penetration testing must be put in place. Automated vulnerability scanners are available to scan a host or group of hosts on a network for application, network, and operating system vulnerabilities. Penetration testing, on the other hand, is a process that is designed to attempt to compromise the security of a host or network using the tools that an attacker would likely use (Tracy, Jansen, & McLamon 2002). Vulnerability scanning should be conducted periodically, at least daily to weekly, and penetration testing should be conducted at least quarterly (Prescatore 2003).

Securing the Web Server Applications

The general principles of this process will be very similar to those of the process for securing the operating system. I will continue to follow the basic guideline that only the minimum amount of services should be installed that are necessary for the Web server to perform its role (Tracy, Jansen, & McLamon 2002). In addition to this, patches and upgrades should be deployed so that known vulnerabilities can be eliminated. During the installation of the Web server, the following steps should be performed:

1. Install the server software on a dedicated host
2. Install the minimum Internet Services required
3. Apply any patches or upgrades to correct for known vulnerabilities
4. Create a dedicated physical disk or logical partition (separate from operating system and server application) for Web content
5. Remove or disable all services installed by the Web server application but not required
6. From the Web server application root directory, remove all files that are not part of the Web site
7. Remove all sample documents, scripts, and executable code
8. Remove all vendor documentation from server
9. Apply appropriate security template or hardening script to server
10. Reconfigure HTTP service banner (and others as required) NOT to report Web server and operating system type and version.

LISTING 10 – (Tracy, Jansen, & McLamon 2002)

The Web server processes should have read-only access to only the files that are necessary for the processes to perform their jobs (Tracy, Jansen, & McLamon 2002). Use Web server host operating system access controls to enforce the following:

- Web service process(es) is (are) configured to run as a user with a strictly limited set of privileges (i.e., not running as root, Administrator, or equivalent).
- Web content files can be read but not written by Web service process(es).
- Web service process(es) cannot write the directories where public Web content is stored.
- Only process(es) authorized for Web server administration can write Web content files.
- The Web server application can write Web server log files, but log files cannot be read by the Web server application. Only root/system/administrative level processes can read Web server log files.
- Temporary files created by the Web server application, such as those that might be generated in the creation of dynamic Web pages, are restricted to a specified and appropriately protected subdirectory.
- Access to any temporary files created by Web server application is limited to the Web service process(es) that created these files.

LISTING 11 – (Tracy, Jansen, & McLamon 2002)

A specified directory or drive should be dedicated to Web content and the Web server application should not be able to access or save files outside of that area (Tracy, Jansen, & McLamon 2002). Links or shortcuts in the public Web content file structure should not point to files or directories outside of this area (Tracy, Jansen, & McLamon 2002). Log files should be stored on a separate, secure host; they should not be stored on the Web server and especially not within the Web content file structure (Tracy, Jansen, & McLamon 2002). The following steps are required to restrict access to a specified Web content file directory tree:

- Dedicate a single hard drive or logical partition for Web content and establish related subdirectories exclusively for Web server content files, including graphics but excluding scripts and other programs.
- Define a single directory exclusively for all external scripts or programs executed as a part of Web content (e.g., CGI, Active Server Page [ASP], Hypertext Preprocessor [PHP]).
- Disable the execution of scripts that are not exclusively under the control of administrative accounts. This action is accomplished by creating and controlling access to a separate directory intended to contain authorized scripts.
- Disable the use of hard or symbolic links.
- Define a complete Web content access matrix. Identify which folders and files within the Web server document are restricted and which are accessible (and by whom).

LISTING 12 – (Tracy, Jansen, & McLamon 2002)

Securing the Web Content

In Web security, one area that is often overlooked is the security of the actual Web content itself. Web content security has two elements. The first element is to be sure that proprietary, confidential, and classified information is not accessible to the public (Tracy, Jansen, & McLamon 2002). The second element of Web content security is in securing the way that particular types of content are processed on the Web server

(Tracy, Jansen, & McLamon 2002). Failure to address this element could result in the compromise of the Web server.

As a rule, never use a public Web server to host sensitive information that only internal users will need to be able to access. To ensure a consistent approach, an organization should create a formal policy and process for determining and approving the information to be published on a Web server (Tracy, Jansen, & McLamon 2002). This process or policy should help to determine what type of information should be published openly, what information should be published with restricted access, and what information should not be publicly accessible at all. Such a process should include the following steps:

1. Identify information that should be published on the Web
2. Identify the target audience (why publish if no audience exists?)
3. Identify possible negative ramifications of publishing the information
4. Identify who should be responsible for creating, publishing, and maintaining this particular information
5. Create or format information for Web publishing
6. Review the information for sensitivity and distribution/release controls (including sensitivity of the information in aggregate)
7. Determine the appropriate access and security controls
8. Publish information
9. Verify published information
10. Periodically review published information to confirm continued compliance with organizational guidelines.

LISTING 13 – (Tracy, Jansen, & McLamon 2002)

This policy should also address information that can be viewed in the source code of a Web page as this can be viewed by any Web browser. A public Web site should generally not contain the following information:

- Classified records
- Internal personnel rules and procedures
- Sensitive or proprietary information
- Personal information about an organization’s personnel
    - Home addresses and phone numbers
    - Social Security Numbers
    - Detailed biographical material (could be employed for social engineering)

    - Staff family members
- Telephone numbers, e-mail addresses, or general listing of staff unless necessary to fulfill organizational requirements
- Schedules of organizational principals or their exact location
- Information on the composition or preparation of hazardous materials or toxins
- Sensitive information relating to homeland security
- Investigative records
- Financial records (beyond those already publicly available)
- Medical records
- Organization's physical and information security procedures
- Information about organization's network and information system infrastructure
- Information that specifies or implies physical security vulnerabilities
- Plans, maps, diagrams, aerial photographs, and architectural plans of organizational building, properties, or installations
- Information on disaster recovery or continuity of operations plans except as absolutely required
- Details on emergency response procedures, evacuation routes, or organizational personnel responsible for these issues
- Copyrighted material without the written permission of the owner
  Privacy or security policies that indicate the types of security measures in place to the degree that they may be useful to an attacker

LISTING 14 – (Tracy, Jansen, & McLamon 2002)

The next area that should be addressed when securing the content of a Web server is Active content. Active content refers to interactive elements that are processed by the client (Tracy, Jansen, & McLamon 2002). If these elements are not developed with security in mind, they can present a serious threat to the user. Organizations that are considering deploying active content should do a risk assessment to determine if the benefit outweighs the risk to the clients as well as the Web server (Tracy, Jansen, & McLamon 2002).

Another consideration when using Active content is that content generators must be implemented on the Web server side. These can be threats to the Web server as well. Specifically, the content generators accept input from users and then take actions on the Web server or back-end databases. If security was not considered during the programming, attacks such as buffer overflow attacks or SQL injection attacks can be used to compromise the Web server. With this in mind, security should be involved with each stage of the development so that scripts can be written to protect against these attacks. Ideally, server-side scripts should restrict users to a defined set of actions and validate the size and values of the input that is provided by the client. All scripts should be run with the principle of least privilege; this will add security in the event of a buffer overflow or SQL injection attack (Tracy, Jansen, & McLamon 2002). In addition to this, the location of active content should be taken in to consideration. Follow these guidelines when placing the Web content:

- Writable files should be identified and placed in separate folders. No script files should exist in writable folders. As an example, guest book data is usually saved in simple text files. These files need write permissions for guests to be able to submit their comments.
- Executable files (e.g., DGI, .EXE, .CMD, and PL) should be placed in separate folder(s). No other readable or writable documents should be placed in these folders.
- Script files (e.g., ASP, PHP, and PL) should have separate folder(s).
- Include files (e.g., INC, SHTML, SHTM, and ASP) created for code reusability should be placed in separate directories. SSI should not generally be used on public Web servers. ASP include files should have an .asp extension instead of .inc. Note much of the risk with include files is in their execute capability. If the execute capability is disabled this risk is drastically reduced.

LISTING 15 – (Tracy, Jansen, & McLamon 2002)

Administration of the Web Server

Once the Web server is setup, proper administration of the Web server is a key element to Web server security. Administrators should be sure that the Web server is logging the appropriate data. In addition to this, it is imperative that these logs are monitored and analyzed regularly. Logs can often be the only record of malicious activity. Web server logs can provide the following information:

- Alerts to suspicious activities that require(s) further investigation
- Tracking of an intruder's activities
- Assistance in the recovery of the system
- Assistance in the post-event investigation
- Required information for legal proceedings

LISTING 16 – (Tracy, Jansen, & McLamon 2002)

The frequency at which the logs are reviewed will depend on the following factors:

- Traffic the server receives
- General threat level
- Specific threats (at certain times specific threats arise that may require more frequent log file analysis as a result)
- Vulnerability of the Web server
- Value of data and services provided by the Web server

LISTING 17 – (Tracy, Jansen, & McLamon 2002)

In addition to the regular monitoring and analyzing that is essential for logging to be effective, analysts should also use logs to compare trends over the course of a longer span of time (Tracy, Jansen, & McLamon 2002). A typical attack can involve hundreds of unique requests that are spread out over a longer period and it may not be possible to recognize this type of attack by viewing a day or week's log files (Tracy, Jansen, & McLamon 2002). It is important to protect log files so that if an attack does occur, the attacker will not be able to modify the logs and erase records of the actions that they took. It is recommended that logs are stored on a separate host from the Web server(s) and a local copy be kept as a backup in case data is lost in transmission (Tracy, Jansen, & McLamon 2002). Logs should be backed up on a regular basis and archived according the organization's records and retention policy.

Data integrity is an important concern in Web server security. Web servers are more exposed to malicious actions than most other servers on an organization's network (Tracy, Jansen, & McLamon 2002). In order to lower the impact of such an attack, a regular backup of the Web server should be done. This is essential so that data can be restored in the event that an attacker compromises the Web server or there is a hardware failure. In addition to a regular backup of the Web server, the Web administrator should keep an authoritative copy of the Web content (Tracy, Jansen, & McLamon 2002). This copy should be located on a separate host and should be located within the internal network of the organization, not in the DMZ (Tracy, Jansen, & McLamon 2002). This authoritative copy of the Web site allows an organization to recover much more quickly from an attack such as Web site defacement but this is not a replacement for regular backups of the Web server (Tracy, Jansen, & McLamon 2002). To ensure the integrity of a Web site using an authoritative copy, take note of the following requirements:

- Protect authoritative copy from unauthorized access
    - Use write once media (appropriate for relatively static Web sites)
    - Locate host with authoritative copy behind firewall, and ensure there is no outside access to host
    - Minimize users with authorized access to host
    - Control user access in as granular manner as possible
    - Employ strong user authentication
    - Employ appropriate logging and monitoring procedures
    - Consider additional authoritative copies at different physical locations for further protection.
- Establish appropriate authoritative copy update procedures
    - Update authoritative copy first (any testing on code should occur before the authoritative copy)
    - Establish policies and procedures for who can authorize updates, perform updates, and when updates can occur, etc.
- Establish a process for copying authoritative copy to a production Web server
    - Data can be transferred using a secure physical media (e.g., encrypted and/or write once media such as a CD-R)
    - Use a secure protocol (e.g., SSH) for network transfers
- Include the procedures restoring from the authoritative copy in the organizational incident response procedures
- Consider automatic updates from authoritative copy to Web server periodically (quarter hourly, hourly, daily, etc.) because this will overwrite a Web site defacement automatically.

LISTING 18 – (Tracy, Jansen, & McLamon 2002)

It is recommended that organizations maintain a development Web server and a QA Web server. These servers should have the same hardware and software as the production Web server. The development and QA Web servers should be located on the organizations internal network. Some examples of how the organization can benefit from maintaining development and QA Web servers are as follows:

- Provides a platform to test new patches and service packs prior to application on the production Web server
- Provides a development platform for the Web master and Web administrator to develop and test new content and applications
- Software that is critical for development and testing that might represent an unacceptable security risk on the production server an be installed on the development server (e.g., software compliers, administrative tool kits, remote access software)

Note: The development and QA Web servers should be separate from the server that maintains an authoritative copy of the content on the production Web server.

LISTING 19 – (Tracy, Jansen, & McLamon 2002)

As part of Web server administration, there should be a process in place for what should be done in the event of a successful attack on the Web server (Tracy, Jansen, & McLamon 2002). The process should provide guidelines for what steps should be taken to respond to a successful attack on the Web server. The process should be precise, showing not only the actions that must be taken, but also showing the order of the actions. Web administrators should take the following steps once a successful attack is identified:

- Isolate compromised system(s) or take steps to contain attack so additional evidences can be collected
- Report incident to organization's computer incident response capability
- Consult the organization's security policy
- Investigate other "similar" hosts to determine if the attacker also has compromised other systems
- Consult, as appropriate, with management, legal counsel, and law enforcement expeditiously
- Analyze the intrusion, including:
    - Modifications made to the system's software and configuration
    - Modifications made to the data
    - Tools or data left behind by intruder
    - Data from system logs, intrusion detection and firewall log files
- Restore the system
    - Two options exist:
        - Install clean version of operating system, applications, necessary patches and Web content
        - Restore from backups (this option can be more risky, as the backups may have been made after the compromise and restoring from a comprised back may still allow the attacker access to the system).
    - Disable unnecessary services
    - Apply all patches
    - Change all passwords (even on uncompromised hosts) as required

    - Reconfigure network security elements (e.g., firewall, router, IDS/IPS) to provide additional protection and notification
- Reconnect system to network
- Test system to ensure security
- Monitor system and network for signs that the attacker is attempting to access the system or network again
- Document lessons learned

LISTING 20 – (Tracy, Jansen, & McLamon 2002)

Web server administrators should carefully consider whether to enable the capability to remotely administer and/or update content on a Web server. The most secure configuration is to disallow any remote administration or content updates, although that might not be viable for all organizations. If an organization determines that it is necessary to remotely administer or update content on a Web server, the following steps should ensure secure implementation:

- Use a strong authentication mechanism (e.g., public/private key pair, two factor authentication, etc.)
- Restrict hosts that can be used to remotely administer or update content on the Web server
    - Restrict by IP address (not hostname)
    - Restrict to hosts on the internal network
- Use secure protocols (e.g., SSN, HTTPS, SFTP), not insecure protocols (e.g., Telnet, file transfer protocol [FTP], network file system (NFS) or HTTP). Secure are those protocols that provide encryption of both passwords and data.
- Enforce the concept of least privilege on the remote administration and content updating (i.e., attempt to minimize the access rights for the remote administration/update account[s]).
- Do not allow remote administration from the Internet through the firewall.
- Change any default accounts or passwords for the remote administration utility or application.
- Do not mount any file shares on the internal network from the Web server or vice versa.

LISTING 21 – (Tracy, Jansen, & McLamon 2002)

Conclusion

As the focal point of many attacks and attempts to gain critical information about an organization, Web sites must be an essential part of an organization's security program. Through design, implementation, and administration, each organization must strive to protect its Web site and its organization through the multi-layered defense mechanisms that I have discussed in this paper. Managers and business owners who fail to address this critical piece of their organizational security expose their company to various threats that can have a devastating effect on an organization and its assets.

Erik Evans is a Security Analyst for HCR-Manorcare. He can be reached at eevans@hcr-manorcare.com

Works Cited

Kessler, G. (2000, April). *Web of Worries, Information Security Research Article.* Retrieved January 25, 2006 from http://infosecuritymag.techtarget.com/articles/april00/cover.shtml

Mattsson, U. (2004, January). *A Practical Implementation of a Real-time Intrusion Prevention System for Commercial Enterprise Databases, ITsecurity.com research article.* Retrieved February 24, 2006 from http://itsecurity.com/papers/protegrity2.htm

Prescatore, J. (2003, February). *CIO Alert: Follow Gartner's Guidelines for Updating Security on Internet Servers, Reduce Risks, Gartner Research Article IGG-02122003-02.* Retrieved January 10, 2006 from http://gartner.lib.depaul.edu/gartner_intraWeb/research/113100/113116/113116.html

Secure Computing Corporation (2003, August). *Intrusion Prevention Systems (IPS).* Retrieved February 24, 2006 from http://searchopolis.looksmart.com/pdf/Intru-PrevenWP1-Aug03-vF.pdf

Tracy, M. & Jansen, W. & McLamon, M. (2002, September). *Guidelines on Securing Public Web Servers, NIST Special Publication 800-44.* Retrieved January 25, 2006 from http://csrc.nist.gov/