

# **INTERNET / INTRANET SECURITY POLICY**

IS Team Approval: March 30, 2006, Unanimous w/2 Absent

TAB Review Date: April 17, 2006

TAB Approval Date: May 15, 2006, Unanimous w/8 Absent

Director Approval Date: May 16, 2006

## **OSF Specification:**

### **5.5—Internet / Intranet Security**

The World Wide Web (WWW) is a system for exchanging information over the Internet. An Intranet is a proprietary network that is specific for an entity, such as the State.

At the most basic level, the Web can be divided in two principal components: Web servers, which are applications that make information available over the Internet (in essence publish information) and Web browsers (clients), which are used to access and display the information stored on the Web servers. 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.

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

- A. 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.
- B. Denial of Service attacks may be directed to the Web server denying valid users an ability to use the Web server for the duration of the attack.
- C. Sensitive information on the Web server may be distributed to unauthorized individuals.
- D. Sensitive information that is not encrypted when transmitted between the Web server and the browser may be intercepted.
- E. Information on the Web server may be changed for malicious purposes. Web site defacement is a commonly reported example of this threat.
- F. Malicious entities may gain unauthorized access to resources elsewhere in the organization's computer network via a successful attack on the Web server.
- G. 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.
- H. The server may be used as a distribution point for illegal copies software attack tools, or pornography, perhaps making the organization liable for damages.

The hosting agency is responsible for the Web server. Some examples of controls to protect from unauthorized access or modification are:

- A. install or enable only necessary services,

- B. install Web content on a dedicated hard drive or logical partition,
- C. limit uploads to directories that are not readable by the Web server,
- D. define a single directory for all external scripts or programs executed as part of Web content,
- E. disable the use of hard or symbolic links,
- F. 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), and
- G. use host-based intrusion detection systems and/or file integrity checkers to detect intrusions and verify Web content.

Maintaining a secure Web server is the responsibility of the hosting agency and involves the following steps:

- A. configuring, protecting and analyzing log files,
- B. backing up critical information frequently,
- C. maintaining a protected authoritative copy of the organization's Web content,
- D. establishing and following procedures for recovering from compromise,
- E. testing and applying patches in a timely manner, and
- F. testing security periodically.

A firewall environment **must** be employed to perform the following general functions:

- A. filter packets and protocols,
- B. perform inspection of connections,
- C. perform proxy operations or selected applications,
- D. monitor traffic allowed or denied by the firewall, and
- E. provide authentication to users using a form of authentication that does not rely on static, reusable passwords that can be sniffed.

The hosting agency responsible for Internet security **will**:

- A. Keep operational systems and applications software up to date. Because software systems are so complex, it is common for security-related problems to be discovered only after the software has been in widespread use. Although most vendors try to address known security flaws in a timely manner, there is normally a gap from the time the problem is publicly known, the time the vendor requires to prepare corrections and the time you install the update. This gap gives potential intruders an opportunity to take advantage of this flow and mount an attack on computers and networks. To keep this time interval as short as possible, it is required to stay aware of:
  1. announcements of security-related problems that may apply,
  2. immediate actions to reduce exposure to the vulnerability, such as disabling the affected software and
  3. permanent fixes from vendors.
- B. Restrict only essential network services and operating system on the host server.
  1. Ensure that only the required set of services and applications are installed on the host server. Either do not install unnecessary services or turn the services off and remove the corresponding files (and any other unnecessary files) from the host.
- C. Configure computers for file backup.

- D. Protect computers from viruses and programmed threats.
- E. Allow only appropriate physical access to computers.
- F. Design, implement and monitor an effective firewall system.

## **ODCTE Implementation**

### **5.5—Internet / Intranet Security**

The ODCTE adopts and adheres to this policy in its entirety as stated in the OSF Specifications above, with the exception of two minor word changes in the section listed below.

The hosting agency is responsible for the Web server. Some examples of controls to protect from unauthorized access or modification are:

- E. ~~disable~~ **avoid** the use of hard or symbolic links,
- G. use ~~host-based~~ intrusion detection systems and/or file integrity checkers to detect intrusions and verify Web content.

For assistance with this policy, please contact Computer Support.