GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Information System Security Education, Training, & Awareness for Web Administration – An Integral Part of Defense-in-Depth

Ray Letteer

September 16, 2000

"Teach people correct principles, and they govern themselves."

- Joseph Smith, theologian and philosopher: 1830

Background

When I first became involved with Information system security around 1986, I learned that much of the emphasis by management on computer security was focused primarily on the hardware. Monies and time was inordinately expended on getting the newest piece of hardware, with the most up-to-date piece of software, and build our virtual bastion against intruders. What was forgotten was that any systems are tools and any tool is only as good as the person using it.

Much has been made about Defense-in-Depth, wherein the Department of Defense (DoD), and thereafter, the rest of the federal government, outline the perimeters of a layered defense for information systems. This concept is based on a series of firewalls, filter routers, and proxy servers that is supposed to protect the confidentiality, availability, and integrity of both systems and information. However, I noted that the implementation of Defense-in-Depth, seems to leave out that most important element – the person.

I recommend establishing a standard training program that addresses information system security and information security in the DoD. Due to the broad nature of the functions in DoD Information Assurance, I am limiting my review. I will focus on developing recommendations to identify unique knowledge and skills required for personnel who are involved in the functionalities of administrating DoD information presented on the World Wide Web. This includes the actions of releasing, using, and protecting this information, from decision to display to maintenance of accuracy and availability.

My research included a policy review, with an emphasis placed on guidance issued by the Offices of the Secretary of Defense. This was primarily due to the fact that the Unified and Specified Commands (CINCs), the Services, and the various Defense Agencies have not been able to consolidate an agreed upon set of standards.

I also researched the business and academic environments, where Web site administration research and business implementation is on the cutting edge. These "best practices" and "lessons learned" from experience guided this research to use what works and discard untested speculation, focusing on those situations having parallel applications in the Government environment.

Web Administration Functionalities

In order to determine these training recommendations, the functionalities associated with administrating a Web site had to first be determined. For administering Web services, these fell mainly into three categories: information management, information systems administration, and information systems security.

- The information management functionality covers those responsibilities that are concerned with information content, releasability, accuracy, and legality. Information to be posted on a Web server has to be reviewed by competent authority to assure these concerns are met.

- Information systems administration involves the installation, configuration, testing, and maintenance procedures for system hardware and software with the aim of ensuring the safe, secure and consistent operation of the Web site infrastructure.

- The information system security functionality covers those responsibilities that are concerned with information confidentiality, integrity, and availability. Information transiting the Web in the form of e-mail or e-commerce, should also have the qualities of non-repudiation and authenticity.

Oftentimes some of these functionalities blend, e.g., the accuracy issue of information management and the integrity issue of information system security. In all cases, the concern remains that information posted on a DoD Web server be approved for dissemination, be accurate, be available, and be protected.

© SANS Institute 2000 - 2005 Author retains full rights.

Web Administration Roles and Responsibilities

From these functional areas, the roles and responsibilities of the various individuals could be defined. These roles and responsibilities could be distributed to multiple participants or, as is more often the case in field implementation, concentrated into one or two duty positions. The following individuals were identified as having roles and responsibilities in successful Web site administration:

- User (Audience): This is a group or body of individuals who use the product of disseminated information or participate in a business or information exchange through the Web site.

- A DoD Originating Office: This is the office of primary responsibility for the information content of a Web site. They either have information they wish to distribute or a business/mission enterprise to conduct, and Web dissemination has been decided by this office to be the optimal tool. They take the central role determining the origination and ownership of content for release. They also assure the information is reviewed and approved by the Public Affairs Officer.

- Public Affairs Officer: The individual responsible for reviewing, and approving of content for release of DoD information to the public.

- General Counsel: An attorney with the responsibility for the legal review, interpretation, legal counsel, and guidance to the organization wishing to release information through a Web site. If needed, this is the where the Public Affairs Officer will turn to resolve potential legal issues which may arise with information dissemination or information use.

- Web Administrator: A subset of System Administration, in which the primary function is to manage and maintain a particular Web site. Depending on the organizational structure, duties could include: Content Design, Database Management, and Web Server Security.

- Systems Administrator: The individual responsible for the day-to-day operation of an organizations system. In many cases, the Systems Administrator has the additional duty of Web Administrator.

- Information System Security Officer: The individual responsible for the confidentiality, integrity, and availability of system information and resources. These duties include the protection of Web resources as they impact the information flow and exchange into the organization’s system.

- Designated Approving Authority: The individual with the responsibility and authority to permit the processing of information on a system, at a particular security mode, with a stated level of risk, with approved countermeasures. Oftentimes this is the "owner" of the organization or unit’s system or information.

Certification and Training Efforts

The concern arises in how to offer training of sufficient quality and quantity to these individuals, in their capacity and roles of Web administration. In looking for training currently offered throughout the DoD, I did find that a wide-ranging and comprehensive Information Assurance training effort already exists within DoD addressing security concerns related to the confidentiality, availability, and integrity of systems. These efforts are conducted by most elements and at all levels of the Department.

DoD is currently developing a standard for certification of System Administrators to establish core competency and professional standards. A similar certification does not exist for Webmasters as a separate entity on a Department-wide basis.

The Defense Information Systems Agency/Information Assurance Program Management Office (DISA/IPMO) has developed "Designated Approval Authority Basics", "Operational Information Systems Security" and "DoD INFOSEC Awareness" courses. These courses are taught through computer-based training and are used by many organizations as the basis for level one System Administrator certification.

However, there is too much diversity in content of courses touted as relating to Web Administration, Web Management, and Web Security. Consequently, there is no clear track of instruction for individuals involved in any of the three Web administration functionalities to receive comprehensive training or detailed education. In particular, there is an alarming lack of emphasis in any training on the information management skills for those individuals required to fulfill that functionality in Web administration.

© SANS Institute 2000 - 2005 Author retains full rights.

Recommendations:

Identify a Common Core of Knowledge. A distinction can be made between core principles and knowledge. In examining current security education efforts, core principles can be identified regarding the safeguarding and protection of classified and sensitive information. Most of these principles deal with problems of access and the steps taken to discourage unauthorized attempts, prevent inadvertent release, or assure adequate safeguarding. As stated above, these principles are already articulated throughout DoD in Information Assurance efforts such as briefings, presentations, programs, courses, and documents. The Joint Staff has recently completed an outline of many of the specific tasks and skills required by individuals in various roles within System Administration. These tasks and skills should be drawn from and incorporated into a formal requirement of Knowledge, Skills, and Abilities in which to measure potential participants in various roles of Web administration.

Certification. A uniform certification process should be developed and maintained for all Web administrator functions in the Department. The technical and security skills can be a subset of the System administration requirements, but they should be distinctive in focusing on operating a Web server. For individuals with the combined responsibility of Web administration with System administration, this certification should consist of obtaining a level one certification for system administration prior to assuming Web administration duties. System Administrators for those organizations which maintain publicly accessible Web sites should receive a level two Web Administrator certification, when defined by the DoD. This is to assure their capability of implementing Web server and firewall resources; and that they implement and maintain appropriate safeguards for the network. These certifications should be renewed at least annually, and include practical demonstrated skills evaluation, to assure currency of Web and System administrator functions with changing technologies. Documented continuing education can be used to constitute portions of re-certification. Similar requirements should be made for contractor personnel employed by the Department. These requirements may be included in contractual agreements and documentation.

Consolidate Current Training Resources in the Department. The Information Assurance training effort should be consolidated on a Department-wide basis to promote currency, quality, and the transmission of "best practices" and "lessons learned." Too many service elements and agencies are attempting to "reinvent the wheel" in information system administration and security. Efforts should be made to collect these and combine them into DoD accepted practices, then distribute them to the CINCs, services, and agencies within the Department. These practices can then be refined by adding any additional requirements from the rest of the Department. The should be managed through the Defense Information Assurance Program (DIAP) office. As outlined in Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6510.01B, Annex C, the responsibility of providing this level of training has been delegated to the DISA/IPMO Education, Training, Awareness, and Products branch (D253).

A major consideration in designing future information system security training programs focusing on Web servers is to take into account not only the technical and security functions of Web administration, but also the audience or internal customers. The Internet environment in which DoD personnel find themselves is constantly changing. This is due to the rapidity of technological change that is placing the capabilities of presenting information in Web formats directly in the hands of the information holder or content manager.

The traditional paradigm of the Webmaster and technical support personnel providing the medium for the expression of content is becoming obsolete. The consequence of these developments is manifold. Future training programs must address not only content-oriented security issues with the information holder, but technical questions as well. Education and the medium through which it is delivered must be able to conform to the evolving technological environment to remain applicable and relevant.

References

Office of the Assistant Secretary of Defense memorandum. *"Web Security Administration*". December 7, 1998

DOD Directive 5122.5. "*Assistant Secretary of Defense for Public Affairs Office*". March 29, 1996

DOD Directive 5400.7. "*DOD Freedom of Information Act Program*". September 9, 1997

DOD Directive 5400.18. "*Community Relations*". June 10, 1976

DOD Directive 5230.9. "*Clearance of DOD Information for Public Release*". April 9, 1996

DOD Instruction 5230.29. "*Security and Policy Review of DOD Information for Public Release*". May 6, 1996

DOD Instruction 5200.40. "*DOD Information Technology Security Certification and Accreditation Process (DITSCAP)*".

© SANS Institute 2000 - 2005 Author retains full rights.

December 30, 1997

DOD Manual 8510.1-M. "*DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Applications Manual*". July 2000

Under Secretary of Defense (P&R) and OASD (C3I) memorandum. "*Information Assurance (IA) Training and Certification*". June 29, 1998.

NSTISSI No. 4009. "*National Information Systems Security (INFOSEC) Glossary*", August 1997

Public Law 100-235. "*Computer Security Act of 1987*"

44 USC Chapter 35. "*Paper Reduction Act*" as amended

© SANS Institute 2000 - 2005, Author retains full rights.