



MICHAEL MILLER INSURANCE

SINCE 1977

Tips for Enhancing Security of Web Servers (Web Sites)

The following list provides a few suggestions that may improve a web site's security posture. These practices are not intended to be a complete listing of security enhancement measures, and there is no assurance that, if followed, a web site will not be compromised, defaced, or otherwise attacked or disabled.

Server configuration

- Configure web server on a host computer dedicated to web server functions; remove all unnecessary services, applications, administrative tools, accounts, pages, files, and directories; change default passwords.

Data and file security

- Do not store source code or data on web server; limit the files that can be uploaded; restrict access to directories and administrative tools; regularly review content exposed on the web server; maintain authoritative copies of content and application code in a separate secure location; utilize encryption to protect sensitive information transmitted over the Internet.

Identity and access management

- For interactive websites, require users to provide unique identification (such as user ID and password); configure user accounts to access only the information that is necessary to complete the approved function or transaction.

Physical security and maintenance

- Physically secure and restrict physical access to the web server; backup the web server on a frequent basis; keep web server current with recommended security patches for the version in use.

Perimeter security

- Implement anti-virus software and run regular scans for malicious code; implement a DMZ (demilitarized zone or perimeter network) with appropriate firewall to separate public facing web server from the internal network; implement intrusion detection and prevention software to identify suspicious traffic directed at the web server.

Log management and review

- Review web server security event logs regularly for suspicious activity; maintain copies of security event logs separate from web server long enough to enable future research if a security incident occurs.

Ongoing review and maintenance

- Assess the web server for vulnerabilities on a regular and continuing basis; engage the services of a trusted security consultant to assess the security posture of the web server environment for your specific needs.

There are numerous websites, books, and periodicals that provide helpful information on enhancing security practices. A few are provided below:

1. ISO, International Organization for Standardization, ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612
2. OWASP, Open Web Application Security Project, http://www.owasp.org/index.php/Main_Page
3. SANS (Systems and Network Security), <https://www2.sans.org/>
4. US-CERT United States Computer Emergency Readiness Team, http://www.us-cert.gov/current/current_activity.html
5. Carnegie Mellon Information Security Office, <http://www.cmu.edu/iso/governance/guidelines/web-server.html>
6. CERT (Computer Emergency Response Team), <http://www.cert.org/>

The loss prevention information and advice presented in this brochure are intended only to advise our insureds and their managers of a variety of methods and strategies based on generally accepted safe practices, for controlling potentially loss producing situations commonly occurring in business premises and/or operations. They are not intended to warrant that all potential hazards or conditions have been evaluated or can be controlled. They are not intended as an offer to write insurance coverage for such conditions or exposures, or to imply that Great American Insurance Company will write such coverage. The liability of Great American Insurance Company is limited to the specific terms, limits and conditions of the insurance policies issued.
