

Network Protection for Design Professionals

Configuration Management

Background:

Configuration Management — is a compilation of procedures for keeping track of changes and evaluating changes to hardware, software and network configurations to ensure that changes to the system do not unintentionally or unknowingly diminish security. Seemingly insignificant changes to information systems can have significant impact on the security of those systems. Systems are constantly being scanned and probed by potential intruders for the types of exploitable weaknesses that may be introduced by these changes. Locking down system configuration makes it much more difficult for unauthorized executable files or malicious code to be surreptitiously installed.

How to implement appropriate controls:

A Configuration Management process should be implemented which addresses the following key elements:

- **Configuration Management Policy and Procedures** — addresses purpose, scope, roles, responsibilities, and compliance; and formal, documented procedures to facilitate the implementation of the CM policy and associated CM controls.
- **Documentation of Baseline Configuration** — documented baseline configuration of the information system and an inventory of the system's constituent components.
- **Configuration Change Control** — documentation and control of changes to the information system. Appropriate organization officials should approve information system changes in accordance with organizational policies and procedures which should include separation of duties such that no individual can subvert this process.
- **Monitoring Configuration Changes** — security impact analyses to determine the effects of the changes.

Resources:

Information Security Handbook: A Guide for Managers, Chapter 14, National Institute of Standards and Technology,

<http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>

