DEVICE HARDENING

Implementing CIS Level 1 Hardening Standards to Optimize Security

Sandbox Technologies
4111 West Alameda Avenue, Suite 605
Burbank, CA
www.sandboxtech.com
Tel. 424.207.5130

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Device Hardening

Improve your organization's security by adopting CIS Level 1 device hardening standards.

What is Device Hardening

Simply stated, device hardening is the application of configuration settings, the disabling of non-essential services, and the implementation of best practice security controls. The purpose of device hardening is to aggressively eliminate or mitigate potential threat vectors that could be used to compromise a machine.

The Center for Internet Security (CIS) publishes an extensive list of device hardening standards recommended for computer workstations and servers. Settings may vary from one device to another based on factors including the device's operating system and its purpose (e.g., server or workstation).

Examples of hardening include the disabling of unused protocols, the removal of local administrative capabilities (e.g., disallowing the installation of software by the device's user) and restricting the way in which physical ports can be used. (For example, if a user's job responsibilities do not require the ability to routinely copy company data to external media, USB ports can be restricted to disallow the use of removable media, while still permitting the use of keyboards, printers, etc).

Policy Examples

- Configure devices to lock after 15 minutes of inactivity.
- Require password complexity and mandatory 30-day password changes.
- Enable whole disk encryption.
- Disable unneeded and less secure services and features.
- Do not display previous username at login prompt.
- Disable the ability for local service user to impersonate the Operating System.
- Limit remote actions to administrators only.
- Limit the ability for users to make certain changes that could negatively affect performance or reliability.

Planning and Deploying Device Hardening Configurations

General steps required to implement device hardening standards for an organization include:

- Identification of target computers (i.e., the computer workstations and servers to be hardened).
- Documenting each device's operating system, business purpose, and essential software installed.
- Drafting an action plan outline to include any necessary exclusions for particular devices.
- Meeting with the organization's designated IT contact/approver to present action plan outline, discuss caveats, note revisions and obtain authorization to proceed.
- Edit GPO's to reflect necessary alterations.
- Deploy GPO's and confirm successful deployment.
- Follow up with users and organizational management to identify and implement any additional changes.

For additional information, contact your Sandbox Technologies Engineer, Account Manager or Consulting CIO, or send an email to inquiries@sandboxtech.com.