

7.3.2 Hardening Facts

Hardening is the process of securing devices and software by reducing the security exposure and tightening security controls. Added benefits of improving performance can also happen through the hardening process, but are not the primary goal. The first step should always be to improve the security of the most foundational elements.

You can harden specific hardware devices as well as the software running on the device. The following are recommendations for hardening systems.

- Control login to a system by:
 - Changing default passwords
 - Using complex passwords
 - Requiring multi-factor authentication
 - Using smart cards, finger print readers, text services, or other apps that send verification codes
 - Limit administrative privileges
 - Install only needed software
 - Avoid installing freeware or software from untrusted publishers
 - Install security software such as anti-virus, anti-spyware, anti-rootkit, and firewall.
 - Reduce the attack surface of the device by limiting applications and services running on the device and removing unnecessary software, features, and non-essential services
 - Use role separation by installing services on separate physical systems. If a single system is compromised, only the few services on that system will be affected.
 - Unnecessary services are often installed in new systems by default. Following installation, remove unnecessary services, protocols, and applications.
 - When removing existing services, determine the dependencies of services you are using before altering the system.
 - Examples of non-essential services are TFTP, Telnet and SNMP. DNS, ICMP, and NNTP are generally considered essential protocols and services; however, you should consider the function of your system before leaving them on the system.
 - Identify common configuration baselines that should be applied to all or a group of systems.
 - A *configuration baseline* is a set of consistent requirements for a workstation or server.
 - A *security baseline* is a component of the configuration baseline that ensures that all workstations and servers comply with the security goals of the organization.
 - Use security templates to quickly apply security baseline settings. A *security template* is a saved set of configuration values that produce the system configuration as specified in the configuration baseline. When you apply the security template to a system, the settings within the template are applied to the system. Use security templates to:
 - Quickly apply settings to one or more computers
 - Configure consistent security settings between devices
 - Quickly restore security settings to the baseline
 - Compare the actual settings on a device to the settings required by the configuration baseline
- Microsoft operating systems include the following tools for managing security templates:
- The Security Templates snap-in, which creates and edits templates. Security templates are predefined security settings. You can obtain security templates from various sources, including the NSA, which has predefined settings it believes are appropriate for Windows operating systems.
 - The Security Configuration and Analysis snap-in, which compares the existing settings with the template or applies a template to a single device.
 - The Group Policy Editor, which imports a template into Group Policy and apply the template to multiple computers.
- Check that all software has up-to-date licenses. A license compliance violation may open your organization to legal actions and may cause a vital application to cease its functions.
 - Keep operating system and applications at the most current levels by applying updates. There are three types of updates:

| Update Type | Description |
|--------------|--|
| Hotfix | <p>A <i>hotfix</i> is a quick fix for a problem. Normally, you only install a hotfix if you have the specific problem it is intended to fix. Hotfixes are:</p> <ul style="list-style-type: none"> ▪ Typically made to address a specific customer situation and possibly may not be distributed outside that customer organization. ▪ Commonly used to address freshly discovered security holes. |
| Patch | <p>A <i>patch</i> is also a quick fix, but generally more thoroughly tested than a hotfix and designed for a wider deployment. Patches:</p> <ul style="list-style-type: none"> ▪ Include previous hotfixes that the manufacturer has thoroughly tested for mass deployment. ▪ Include fixes that should be applied to wider audiences, like patching security holes. <p>The best place to obtain updates is from the manufacturer's website.</p> |
| Service Pack | <p>A <i>service pack</i> (SP) is a collection of patches, hotfixes, and other system enhancements that have been tested by the manufacturer for wide deployment. A service pack includes all previously released bug fixes. If you install the service pack, you do not need to install individual patches. Installing a service pack also includes all previous service packs.</p> |

When managing updates, be aware of the following:

- Patch management activities include:
 - Determining which patches are needed on the system
 - Testing patches in a lab environment to identify the effects of applying the fixes
 - Applying the patches
 - Auditing for successful application of patches
- Use patch management software to simplify the patch distribution and management process. Windows Software Update Services (WSUS) is a patch management tool that allows clients on a network to download software updates from a WSUS server internal to their organization.
 - The WSUS server receives a list of available updates from Microsoft.
 - On the WSUS server, you identify allowed or required patches for your organization.
 - Clients download only approved patches from an internal WSUS server or directly from Microsoft.

You can also use Group Policy to distribute and automatically install patches. You must use Group Policy to install updates to non-Microsoft software that is not supported by WSUS.

- You do not necessarily need to install every hotfix, patch, or service pack that is released. For example, if a hotfix applies to a service that you have disabled on your servers, applying that hotfix is not required. Or if a patch applies to browser security and the browser on the server is not used, the patch will not need to be applied.
- Be sure to test patches before applying patches within your organization. A common strategy is to:
 1. Apply and test patches in a lab environment.
 2. Deploy patches to a set of systems, such as a single department.
 3. Deploy patches system-wide.

A Trusted Operating System (TOS) is an operating system that comes hardened and validated to a specific security level as defined in the Common Criteria for Information Technology Security Evaluation (CC). Many TOSs provide sufficient support for *multilevel security*, where multiple levels of classified data reside within the same system, but users are not permitted to access data at different classification levels. Additionally, all personnel must have access approval on a need-to-know basis.

Most organizations maintain a Standard Operating Environment (SOE) which is implemented as a standard disk image or master image. This disk image is used when deploying new computers to the network. Automation is used when deploying the master image and when running configuration scripts, to give the computer a name, to join a domain, and during any other customizations. The use of a master image and automation can reduce security risks by ensuring that security standards are consistent throughout the network. Master images should be based on a TOS and be fully patched.

TestOut Corporation All rights reserved.