National Cyber Security Centre
a part of GCHQ

Guidance (/)

10 Steps: Secure Configuration

Created: 29 Sep 2015
Updated: 08 Aug 2016
Part of: 10 Steps to Cyber Security (/guidance/10-steps-cyber-security)
This section from within the NCSC's '10 Steps To Cyber Security' concerns Secure Configuration.

Summary

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

What is the risk?

Establishing and actively maintaining the secure configuration of systems should be seen as a key security control. Systems that are not effectively managed will be vulnerable to attacks that may have been preventable. Failure to implement good configuration and patch management can lead to the following risks:

- **Unauthorised changes to systems:** The protections you believe you have in-place may be changed by unauthorised individuals, either internal or external, leaving information at risk.
- **Exploitation of software bugs:** Attackers will attempt to exploit unpatched systems to provide them with unauthorised access to system resources and information. Many successful attacks exploit vulnerabilities for which patches have been issued but not applied.
- **Exploitation of insecure system configuration:** An attacker could exploit a system that has been poorly configured by:
-
  - gaining access to information they are not authorised to see
  - taking advantage of unnecessary user rights or system privilege
  - exploiting unnecessary functionality that has not been removed or disabled
  - connecting unauthorised equipment that is then able to compromise information or introduce malware
  - creating a back door to use in the future for malicious purposes

How can the risk be managed?

Organisations need to ensure that they have put in place measures to minimise the risk of poor system configuration. The following security controls should be considered:

Use supported software: Use versions of operating systems, web browsers and applications that are vendor (or community) supported.

Develop and implement policies to update and patch systems: Implement policies to ensure that security patches are applied in an appropriate time frame, such a 14 days for critical patches. Automated patch management and software update tools might be helpful. In cases where it is not possible to patch a vulnerability steps should be taken to make it very difficult to exploit. This might include making it difficult for an attacker to communicate with the system.

Create and maintain hardware and software inventories: Create inventories of all authorised hardware and software used across the organisation. Ideally the inventory should capture the physical location, business owner and purpose of hardware together with the version and patch status of all software. Tools can be used to help identify unauthorised hardware or software.

Manage your operating systems and software: Implement a secure baseline build for all systems and components, including hardware and software. Any functionality or application that does not support a user or business need should be

removed or disabled. The secure build profile should be managed by a configuration control process and any deviation from the standard build should be documented and approved.

Conduct regular vulnerability scans: Regularly run automated vulnerability scanning tools against all networked devices and remedy or manage any identified vulnerabilities within an agreed time frame.

Establish configuration control and management: Implement policies that set out a configuration control and change management process for all systems.

Disable unnecessary peripheral devices and removable media access: Assess the need for access to peripheral devices and removable media. Disable ports and system functionality that does not support a user or business need.

Implement white-listing and execution control: Create and maintain a whitelist of authorised applications and software that can be executed. In addition, systems should be capable of preventing the installation and execution of unauthorised software by employing process execution controls.

Limit user ability to change configuration: Provide users with the permissions that they need to fulfil their business role. Users with 'normal' privileges should be prevented from installing or disabling any software or services running on the system.

Limit privileged user functionality: Ensure that users with privileged system rights (administrators) have constrained internet and email access from their privileged account. This limits exposure to spear phishing and reduces the ability of an attacker to achieve wide system access through exploiting a single vulnerability.

Learn more

- Read our End User Device Security Guidance for recommendations on configuring modern devices.
- Our Approaching enterprise technology(/guidance/approaching-enterprise-technology-cyber-security-mind) with cyber security in mind guidance contains useful guides on a range of technologies which can help to secure your organisation.
- This Vulnerability management guidance(/guidance/vulnerability-management) has pointers on how to ensure problems in software and hardware products don't cause you problems.

Further reading

Vulnerability management(/guidance/vulnerability-management)
Approaching enterprise technology with cyber security in mind(/guidance/approaching-enterprise-technology-cyber-security-mind)

Topics

Design and configuration(/topics/design-and-configuration)
Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No