Device Hardening

Overview

Implementing Device Hardening in a comprehensive, coordinated manner throughout the enterprise makes it more difficult for an attacker to leverage resources and enhances an enterprise's ability to withstand a persistent attack. This document describes how to apply *Privilege Restriction* and *Coordinated Defense*[1] resiliency techniques.

Applying *Privilege Restriction* to Keep the Adversary from Leveraging Resources

Privilege Restriction - restricting privileges required to use cyber resources, and privileges assigned to users and cyber entities, based on the type(s) and degree(s) of criticality and trust respectively, can minimize the potential consequences of adversary activities.

- Privilege Management: Define, assign, and maintain privileges associated with end users and cyber entities (e.g., systems, services, devices), based on established trust criteria, consistent with principles of least privilege.
- Privilege-Based Usage Restrictions: Define, assign, maintain, and apply usage restrictions on cyber resources based on mission criticality and other attributes (e.g., data sensitivity).
- Dynamic Privileges: Elevate or deprecate privileges assigned to a user, process, or service based on transient or contextual factors such as time of access, location, etc.

Priorities for Immediate Action with *Privilege Restriction*

- Configure each service on a component to restrict it to only the necessary ports and protocols.
    - Review mission functions of services and components, and identify which ports and protocols are required and whether network access is required to support those functions. Restrict any unnecessary ports or protocols or network access.
    - Limit functionality and privileges of devices to only that necessary to perform their specified role or function.
- Locate those instances where "super user" privilege is employed, and validate its need; remove if not necessary.
- Restrict connections by enterprise components.
    - Identify and maintain a list of enterprise-approved networks and enterprise components.
    - Modify the configuration of the components so that it may only connect to approved enterprise networks.
- Configure each service separately using virtualization to provide separate processing domains on components (e.g., servers) that provide shared services.
    - For each component, identify all services provided by that component and determine the access and mission requirements.
    - Segregate services using virtualization based on which services require the same access and mission assurance (e.g., provide a virtualized enclave for telecommuters).

Applying *Coordinated Defense* to Share Situational Awareness and Collaborate

Coordinated Defense – managing multiple, distinct mechanisms adaptively and in a coordinated way – can defend critical resources against adversary activities. This requires coordination across organizations regarding privileges identities and

[1] All italicized words are defined in the *Cyber Resiliency Terms and Concepts* document.

roles – both their consistent use and in the event of a compromise. There are two major implementation approaches to coordinated defense.

- Technical Defense-in-Depth: Make use of multiple protective mechanisms, applied at different architectural layers or locations (e.g., application, endpoints, network, and incident response perimeters). These mechanisms should be periodically reevaluated to ensure their efficacy.
- Coordination and Consistency Analysis: Apply processes, supported by analytic tools, to ensure that defenses are applied and cyber courses of action are defined and executed in a coordinated, consistent, and non-disruptive manner.

Priorities for Immediate Action with *Coordinated Defense*

The top priorities for *Coordinated Defense* are:

- Define a strategy that takes mission or business needs into account to ensure that patching does not interfere with critical operations.
    - Create a patch testing process that incorporates risk management for situations where the patches do interfere with business processes.
    - Implement a regular patching schedule that coordinates with other mission and business schedules.
- Before allowing mobile devices to connect to enterprise networks, ensure that they have been patched and configured properly.
    - If necessary, provide a separate protected enclave to support limited connectivity for devices that do not conform to enterprise policies. This is particularly important if the enterprise supports BYOD (bring your own device).
    - Provide validated patching resources that are accessible to systems outside of the protected enclave as well as BYOD.
- Perform an analysis to ensure that security mechanisms are applied consistently across all components.
    - Determine the security requirements for each set of components that has a specific mission function or criticality.
    - Identify the various security mechanisms that are implemented to achieve the security requirements.
    - Ensure that security requirements are consistently met across each set of components with a specific mission function or criticality.

Technique Interactions

Privilege restriction works in conjunction with *Coordinated Defense*. Specifically the Coordinated Defense Coordination and Consistency Analysis method (described above) provides consistency to restricting privilege across the enterprise while minimizing interference with the mission. As one moves deeper into the organization's infrastructure to enclaves containing more sensitive information, only those users and applications that have appropriate privileges are allowed access to these enclaves, and only a very limited number of such users and applications are granted those privileges.

Preparing for the Future

There are various technological, social and business trends that will have impact on the ability to harden devices. "Bring Your Own Device" policies, the increased use of portable/mobile devices and Internet of Things are, to various degrees, disrupting the assumption that an enterprise can mandate and implement configurations, such as privilege restriction, on systems to harden those components.

In order to consistently and effectively harden systems in this changing environment one needs to:

- Ensure that those devices and components the organization owns/controls are designed with appropriate protections (*Coordinated Defense*) and the minimum set of needed privileges (*Privilege Restriction*). In addition virtualization can be used to periodically refresh the software/firmware of the devices/components and reinstall a clean copy of the software/firmware; in so doing this flushes out any foothold the adversary may gained in the device/component.
- Enhance the hardening provided by *Coordinated Defense* and *Privilege Restriction* even more by combining those techniques with *Diversity* and *Dynamic Positioning.* These techniques can disrupt the attack surface, making it more difficult for the adversary to either locate their desired target or apply the malware most appropriate to the target. Taken together these techniques make the attacker's efforts less effective as they cause the adversary to waste time and effort on misaimed attacks.
- Ensure that those devices and components whose configuration the organization does not control, are 1) not allowed access to the organization's infrastructure; 2) only allowed via non persistent mediated services (e.g., SOA); or 3) are isolated (e.g., through a virtual network or an isolated non persistent virtual environment that is temporary or disposable) so as to minimize harm they could inflict on the infrastructure.