Device Hardening:
Making It Harder for Components to Be Compromised

This paper outlines the best practices for #4 Device Hardening.

Planning and Preparation Activities	***Recovery and Reconstitution Activities***
0. Disrupting the Attack Surface	
1. Architect to Protect *2. Secure Administration* *3. Access Control* *4.* ***Device Hardening*** *5. Backup Strategies* *6. Cyber Continuity of Operations (COOP) Planning*	*7. Cyber COOP Execution* *8. Secure Communications* *9. Core Services* *10. Data Recovery Strategies* *11. Forensics* *12. After Action Activities*

The BIG Idea

Locking down or improving the defenses of component systems and services makes the attacker’s job harder.

Cyber Resiliency Goals & Objectives

Device Hardening supports the *Anticipate*[1] goal and the *Prevent* objective.

Design Principles

The design principles for Device Hardening will improve the defenses of component systems and services, and thus make the adversary work harder.

- *Privilege Restriction*: Minimize the ability of a compromised service within a component to compromise other services on that component and spread to other components. Limit the services between components.
- *Coordinated Defense*: Define a strategy that identifies and isolates unpatched components. Apply security mechanisms consistently across the enterprise.

What Can Be Done Now

Apply standards of good practice for privilege restriction, patching, and configuration management to all components of the enterprise architecture.

- *Privilege Restriction*
  - Configure each service on a component to restrict it to only the necessary ports and protocols.
  - Limit connections to devices and services to those that are pre-authorized.
  - Configure each service separately using virtualization to provide separate processing domains on components (e.g., servers) that provide shared services.
- *Coordinated Defense*
  - To ensure that patching does not interfere with critical operations, define a strategy that takes mission or business needs into account.
  - Before allowing mobile devices to connect to enterprise networks, ensure that they have been patched and configured properly.

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

Approved for Public Release. Distribution Unlimited. Case Number 15-3300. ©2015 The MITRE Corporation. All Rights Reserved.

  - Ensure that security mechanisms are applied consistently across all components.

The Right People & Policies

- Create policies and supporting processes for denying (or limiting) access to enterprise networks from devices that fail to comply with standards for patching and configuration.
- Create policies and processes for coordination among security administrators, cyber defenders, and mission/business process owners to ensure that patching and configuration does not interfere with critical operations.

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques, *coordinated defense* and *privilege restriction*, as described above, defenders can impede the adversary's attack on the enterprise and limit the damage the malware causes. The use of *coordinated defense and privilege restriction* impede the adversary's ability to initiate and exploit malware, employ mechanisms to manage the initial victims, execute the attack plan, and maintain their presence in the enterprise. In addition, *privilege restriction* limits the adversary's ability to execute the attack plan and maintain their presence.

Synergies and Barriers

Synergies among practices include *Privilege Restriction's* use of *Coordinated Defense* (consistency analysis) to ensure consistent privilege management and privilege based usage restrictions.

Barriers to adoption include the following:

- System administrators and mission/business process owners may feel cultural resistance to coordinating together.
- Patching or configuration changes may have unforeseen effects and cause inconvenience or interrupted service. This comes into conflict with the business need of zero downtime.
- Lack of configuration guidance and failure to minimize the attack surface of new devices.

Just Ahead

The growing convergence of enterprise systems and the Internet of Things technologies will increase the importance of locking down all devices that connect to enterprise networks as well as maintaining an awareness of, and treating appropriately, those devices that can't be locked down. Use virtualization technology to periodically refresh system components (*non-persistence*) to flush out adversary foothold in the organization and to dynamically change applications and operations systems (*diversity*) or reposition key assets (*dynamic positioning*) thus causing adversary attacks to be misdirected and wasted.

[2] The Cyber Attack Lifecycle is described in the *Cyber Attack Lifecycle and Resilience* document.

Approved for Public Release. Distribution Unlimited. Case Number 15-3300. ©2015 The MITRE Corporation. All Rights Reserved.