Access Control:
Constraining What the Adversary Can Do

This paper outlines the best practices for #3 Access Control.

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

The BIG Idea

Use access control mechanisms to constrain the actions adversaries can take and and ensure that they are effectively limiting harm, while still allowing legitimate users to continue mission or business functions.

Cyber Resiliency Goals & Objectives

Access control supports the *Anticipate*[1] and *Withstand* goals and the *Constrain* and *Prevent* objectives.

Design Principles

The design principles for access control improve the ability of component systems and services to constrain an adversary's actions, making it harder for the adversary to attack the organization's crown jewels (e.g., critical applications and data stores).

- *Privilege Restriction*: Minimize the number of services and privileges associated with authorized subjects (e.g., users, platforms, services, and applications) based on roles and groups. By restricting the actions subjects can take when they access resources, you can limit the harm an attacker can achieve.
- *Coordinated Defense*: Use a layered, defense-in-depth strategy that requires potential adversaries to navigate through and overcome various access control checkpoints to reach their ultimate objective.
- *Segmentation*: Establish separate domains for critical data and assets. That way, an access compromise in one domain does not affect another.
- *Analytic Monitoring*: Continuously monitor on-going activities to ensure that required access control mechanisms and settings are in place, are operating correctly, and haven't been comprised.

What Can Be Done Now

To maximize the effectiveness of Access Control, apply the following resiliency techniques.

- *Privilege Restriction*

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

  - Configure each service on a component and restrict it to using only the necessary ports and protocols.
  - Minimize or eliminate "super-user" privileges of services.
  - Ensure privileges are employed only by authorized users.
- *Coordinated Defense*
  - Complement organization firewalls with host-based firewalls on desktops/laptops.
  - Define roles and conditions required for accessing or using resources based on organizational policy, and then check that each enforcement mechanism (e.g., on a shared server, for a database) uses those roles and applies those conditions consistently.
- *Segmentation*
  - Use subnets (e.g., DMZs) to logically/physically separate externally facing systems from internally facing systems.
  - To prevent adversaries from gaining access, logically/physically isolate the organization's computer network defenses from critical operational processing networks.
  - Protect and secure highly valuable resources.
- *Analytic Monitoring*
  - Employ continuous monitoring to ensure that required access control measures are in place at each segmentation barrier.

The Right People & Policies

- Move away from a traditional architecture, where protection is primarily at the boundaries of the organization. Instead, layer protection throughout.
- Employ policies and supporting processes to facilitate this transition.

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques, *analytic monitoring*, *coordinated defense*, *privilege restriction,* and *segmentation,* as described above, defenders can detect the adversary, impede the adversary's attack on the enterprise and limit the damage the malware causes. The use of *coordinated defense, privilege restriction,* and *segmentation* impede the adversary's ability to initiate the exploit. The use of *analytic monitoring* enables the defenders to detect the adversary's efforts after this initial exploitation. When the adversary attempts to control the initial victims both *privilege restriction* and *segmentation* limit and impede these efforts*. Coordinated defense* in concert with *privilege restriction* and *segmentation* limit and impede the adversary's ability to execute the attack plan and maintain a presence in the enterprise.

Synergies and Barriers

Synergies among practices include *Coordinated Defense* and *Segmentation*. Barriers to adoption include:

- Cost and administrative issues. Establishing a *coordinated defense* and an in-depth approach to access control requires time, effort, and administrative change.
- Inconvenience and cultural resistance. Even if they do not necessarily need them for their jobs, users may resist losing privileges. Similarly, air gaps are an effective mechanism for *segmentation* if policy and procedures are enforced. The political will as well as administrative resources must be available for this enforcement to work.

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

- Achieving the correct balance in system monitoring. It takes time and effort to tune the monitoring system to detect real access control violations, rather than unintended or mistaken access control attempts.

Just Ahead

The growing convergence of enterprise systems (the “system of systems”) and the Internet of Things technologies will increase the potential adversary attack surface, and further erode the concept of a secure boundary. To address this problem requires increased layering of access control throughout the system. This can be achieved through various means such as virtualization or encryption to separate critical and non-critical resources (*segmentation*) and by requiring dynamically increased level of privileges to access more sensitive information (*privilege restriction*).