Secure Administration:
Securing the Keys to the Kingdom

This paper outlines the best practices for #2 Secure Administration.

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

By using secure system administration and management capabilities, an organization can substantially reduce the opportunities for advanced adversaries to gain elevated privileges and wide-spread network access.

Cyber Resiliency Goals & Objectives

The Secure Administration supports the cyber resiliency *Anticipate*[1] and *Withstand* goals and the *Prevent* and *Prepare* objectives.

Design Principles

The design principles for secure administration create a more resilient enterprise infrastructure by making it more difficult for adversaries and non-administrative users to gain access via unauthorized, privileged actions.

- *Coordinated Defense*: Develop Administrator Standard Operating Procedures (SOPs) in coordination with business operations and Cyber Courses of Action across multiple administrative domains.
- *Privilege Restriction*: Apply good practice standards for least privilege, separation of duties, and role-based access control across administrator accounts; limit administrator account access to non-essential capabilities (e.g., e-mail, Internet).
- *Segmentation*: Designate systems exclusively for administration tasks; physically and logically separate administration and management control channels from the primary enterprise network. As appropriate, further separate activities and functions of privileged users into privileged and non-privileged functions.

What Can Be Done Now

The following resiliency techniques can help transform business processes and redesign systems to use existing technologies more effectively:

- *Coordinated Defense*
    - Ensure that critical resource protections are consistent across the enterprise and are consistent with risk management considerations (i.e., the consequences of a critical resource being compromised)

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

    - Review current administrator SOPs and coordinate security procedures to achieve mission goals.
- *Privilege Restriction*
    - Examine roles, duties and functions to determine the least privilege and function required to perform the mission (for both individuals and systems).
    - Implement changes to enforce principles of least privilege and separation of duties as well as limiting the time for which creditials are valid.
    - Require multi-factor authentication for administrative accounts or any specialized system (e.g., jump station, bastion host) intended to perform some critical security function.
    - Prevent caching administrator credentials.
- *Segmentation*
    - Dedicate specific systems for use only for certain administration tasks.
    - Create an out-of-band management network to administer critical systems.
    - Disallow administration from outside the organization's internal network.
    - Remove all externally facing administration capabilities.

The Right People & Policies

Creating a foundation of resiliency requires specific skills and policies, including:

- Enterprise architects and defenders who understand the risks posed by administrative accounts and privileges.
- System administrators who will do the right thing—even when it is not convenient—to enhance security.
- Strategic planning to ensure that future capabilities are securely administered and monitored.

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques, *coordinated defense*, *privilege restriction,* and *segmentation,* 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, privilege restriction,* and *segmentation* impede the adversary's ability to initiate the exploit. When the adversary attempts to manage the initial victims both *privilege restriction and segmentation* limits and impedes 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 Privilege Restriction and Segmentation. Applying these practices will reduce opportunities for adversaries to gain elevated privileges and wide-spread network access.

- *Privilege Restriction*, by requiring multi-factor authentication for administrator accounts and applying the principles of least privilege.
- *Segmentation*, by physically isolating access to critical systems.
- Virtualization can also augment *segmentation* and *non-persistence*

Barriers to adoption include:

- System administration shortcuts implemented without considering security implications, increase the exposure of administrative channels or privileges.
- Capabilities that do not support secure administration (e.g., no dedicated administration port).

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

- Policies and cultures that favor cost and efficiency over security and resilience.

Just Ahead

Secure administration practices must adjust to emerging technologies. Virtualization, for example, requires both host and guest platforms to be securely administered. Virtual and software-defined networks modify network routing, making management more challenging, while biometrics and new authentication approaches may offer better protection of administrator accounts.