Secure Administration

Overview

Secure system administration and management can substantially reduce the attack surface for the adversary and enable an organization to prevent or withstand an attack for a longer period of time. This document describes how to apply *coordinated defense, privilege restriction* and *segmentation*[1] resiliency techniques.

Applying Coordinated Defense to Strengthen Your Response to the Adversary

Coordinated Defense – managing multiple, distinct mechanisms adaptively and in a coordinated way – can defend critical resources against adversary activities. 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).
- 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 way.

Priorities for Immediate Action with *Coordinated Defense*

The top priorities for *Coordinated Defense* are:

- Coordinate among operators, administrators, and managers of component systems to:
  - Ensure that defenses (e.g., definition of privilege and access) are defined and implemented consistently across component systems and networks.
  - Ensure that Standard Operating Procedures (SOPs) and security procedures are consistent with mission goals.

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

Privilege Restriction - restrict 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, to 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.

Priorities for Immediate Action with *Privilege Restriction*

The top priorities for *Privilege Restriction* are:

- Apply standards of good practice for least privilege, separation of duties, scoped administration (e.g., “just in time admin” and “just enough admin”) and role-based access control

[1] All Italicized words are defined in the Cyber Resiliency Terms and Concepts Document.

    - Trust-based assignment of privileges to users and cyber entities
    - Separate processing domains based on privilege
- Identify critical resources and lock down their use
    - Limit administrator accounts to only the functions they require
    - Ensure that administrator credentials are not cached.
    - Removal of admin rights from end users for their machines.
    - Employ criticality-based restriction of privileges required to use resources.
    - Require dual authorization (i.e., two administrators must authorize an action) for critical functions.
    - Use strong authentication methods to minimize chances of compromise of administrator's authenticators.
        - Strong authentication would include: multifactor authentication to counter credential reuse (e.g., replay attacks), adaptive authentication as more privileged actions are required, periodic re-authentication of administrators, and out of band authenticators to counter impersonation attacks.
- Manage passwords effectively
    - Ensure that good password polices have been established and implemented for both administrative and privileged accounts.
    - Enforce regular password changes for all administrative and privileged accounts.
    - Ensure that administrative and privileged account passwords are unique.
- Seek alignment between business and IT stakeholders on appropriate use of shared services.

Applying *Segmentation* to Isolate the Adversary

Segmentation – physical or logical separation or isolation of resources based on trustworthiness and criticality – can limit the spread of destructive malware in an enterprise information infrastructure. Separation or isolation can be physical or logical, and predefined or dynamic.

- Physical Segmentation: Maintain physically separate devices and networks.
- Logical Segmentation: Separate devices, networks, services, and data repositories using encryption and access control mechanisms.
- Predefined Segmentation: Define enclaves (including separate Active Directory elements), segments, or other types of resource sets based on criticality and trustworthiness, so that they can be protected separately and, if necessary, isolated.
- Dynamic Segmentation/Isolation: Change the definition of enclaves or protected segments, or isolate resources, while minimizing operational disruption.

Priorities for Immediate Action with *Segmentation*

The top priorities for *segmentation* are:

- Implement *segmentation* by removing unnecessary connectivity
    - Dedicate secure systems for use only for certain administration tasks and deny administrators remote access forcing them to administer the machines at the console.
    - Only allow administration of an organization's network from an approved set of devices.
    - Remove any externally facing administration capabilities.

Technique Interactions

Synergies exist between *Privilege Restriction* and *Coordinated Defense* and between *Privilege Restriction* and *Segmentation*. *Coordinated defense* coordinates the use of *privileges* at different locations and layers and *Segmentation* helps limit the scope of a privilege to a defined set of cyber resources.

Preparing for the Future

In addressing Secure Administration for the future, there is a need to consider both technical and non-technical challenges and changes.

Secure administration practices must adjust to emerging technologies. This includes both the challenges such new technology may impose and benefits it may offer. 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. Virtualization also supports the ability to support dynamic, logical segmentation of resources. Using virtualization provides the ability for users to operate in encapsulated virtual environments with just the privileges that they need. Cloud computing is becoming increasingly common. Whether the system administration is provided by the Cloud provider or by the enterprise's administrators, the administration policies should be reviewed to ensure compliance with risk management stance and enterprise policies.

From a non-technical perspective it is important to recognize that the changing and growing threat environment will require personnel to operate somewhat differently than they have in the past. This may require greater coordination and understanding of personnel working in different part of the organization or with different responsibilities within the organization. *Coordinated Defense* would require greater coordination between operators, administrators and managers of component systems in order to consistently defend against and recover from attacks. This coordination enables an organization to apply the defenses at the most effective points and keep critical resources functioning through adverse events. As mission and business processes evolve, and as more information about the adversary becomes available, operators, administrators and managers of component systems need to maintain an ongoing dialog with each other.

Similarly*, Privilege Restriction* requires a shared understanding across all levels of the enterprise in order to ensure systems are securely administered and monitored as the mission, the environment and policies evolve. This requires Enterprise architects and defenders who understand the risks posed by administrative accounts and privileges. A thorough review of systems to identify excessive capabilities and privileges should be performed on a regular basis – as environments evolve privilege and capability creep frequently occur and without a regular review these can provide unneeded capabilities an adversary may use as attack vectors.

Finally, *segmentation*, requires system administrators who are willing to do the right thing even when it is not convenient to enhance security. This understanding and willingness requires the appropriate incentives and training.