Access Control

Overview

Implementing Access control in a comprehensive, coordinated manner throughout the enterprise enables resilience-enhancing practices and techniques to be integrated so that they enhance an enterprise's ability to withstand a persistent attack. This document describes how to apply *privilege restriction, coordinated defense, segmentation*, and *analytic monitoring*[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.

Priorities for Immediate Action with *Privilege Restriction*

- Configure and restrict services on components
  - Assign privileges to users and cyber entities based on the trust level in the cyber entity and user.
  - Use of thin clients for specific functions and associate the appropriate privileges with the client.
  - Separate processing domains based on privilege.
- Minimize or eliminate "super user" privileges
  - Identify critical resources and restrict privileges required to use such resources based on the criticality of the resource.
  - Remove administrator rights from end users for their machines.
  - Locate those instances where "super user" privilege is employed, and validate its need; remove if not necessary.
  - As feasible convert super user privileges to a series of related, role-based, privileges.
- Ensure privileges are employed only by authorized users
  - Implement dual authorization for critical functions.
  - Use strong authentication methods to minimize chances of compromise of administrator's authenticators.
    - Strong authentication would include: multifactor authentication to counter replay attacks, adaptive authentication as more privileged actions are required, periodic re-authentication of administrators, and out of band authenticators to counter man in the middle attacks.

[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.

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 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).
- 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:

- Complement organization firewalls with host/desktop/laptop firewalls
    - Ensure that the policies of the host, desktop, laptop firewalls are defined and implemented consistently with those of the organizational firewall; as feasible employ products from different vendors at the host, desktop and laptop to minimize chance of compromise by adversary.
- 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.
    - Ensure that policies are well defined and in place, and the implementation procedures and user roles are consistent with the policies.
    - Ensure that defenses (in this case, privilege restriction, roles, etc.) are defined and implemented consistently across component systems and networks.

Applying *Segmentation* to Limit Adversary Impacts

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 by limiting the adversary's access. 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:

- Isolate the organization's computer network defenses (CND) from critical operational processing networks.

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

    - Use logical isolation mechanisms (e.g., routers, firewalls, controlled interfaces) to isolate the cyber security operations center (CSOC) or computer security incident response team (CSIRT) enclave from ordinary enterprise operations.
    - Use encryption to protect communications of the CND and other components that support
- Isolate externally facing networks from internally facing resources
    - Use logical isolation mechanisms (e.g., routers, firewalls, controlled interfaces) to isolate the cyber security operations center (CSOC) or computer security incident response team (CSIRT) enclave from ordinary enterprise operations.
- Isolate and secure highly valuable and critical resources (i.e., the organization's crown jewels).
    - Use a combination of predefined segmentation and dynamic segmentation to isolate critical resources
        - Predefined segmentation could be done via defined enclaves and air gaps; best used for those highly critical resources that cannot or should not interface with less sensitive resources.
        - Dynamic segmentation could be done via virtualization and firewalls, best used for resources where some communication between enclave and less critical resources is likely.
    - Validate assumptions about separation or isolation of existing enclaves. These are typically defined based on confidentiality or privacy concerns (e.g., separating personally identifiable information about customers from logistics or other business data), but can also be based on criticality or mission function (e.g., separating a business data subnetwork from a process control network) or trustworthiness (e.g., maintaining a DMZ between the enterprise and the Internet).
        - Analyze the architecture to see where
            - Common resources (e.g., communications media, virtualization servers) are shared across enclaves.
            - Shared services (e.g., SIEM, identity and access management, backup and restore) are provided to protected enclaves.
        - Perform penetration testing or use a red team to determine whether the apparent separation is real, and what the implications of compromise of shared services on protected enclaves are.

Applying *Analytic Monitoring* to Detect Adversary Activity

Analytic Monitoring - gathering, fusing, and analyzing data on an ongoing and coordinated way - can maximize the organization's ability to detect potential adverse conditions, reveal the extent of adversary activity, and identify potential or actual damage to access control mechanisms. This is particularly critical with regard to access control mechanisms. For example, this level of analytic monitoring may reveal attempted access to data, or changes in permissions. There are several implementation approaches to *analytic monitoring*:

- Monitoring and Damage Assessment: Monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity, detect and assess damage, and watch for adversary activities during recovery and evolution.
- Sensor Fusion and Analysis: Fuse and analyze monitoring data and preliminary analysis results from different components, together with externally provided threat intelligence.

Priorities for Immediate Action with *Analytic Monitoring*

The top priorities for *analytic monitoring* are:

- Ensure that the required access control mechanisms are in place and operating correctly
    - Employ IDS at organizational firewall, servers, desktops and laptops.

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

- Analyze data to identify access anomalies (e.g., individuals accessing information they do not normally access or at unusual times)

Technique Interactions

Coordinated Defense and Segmentation provide strong interaction. Defense in depth mechanisms placed at each segment/enclave impose a barrier that adversaries have to overcome. Privilege restriction works in conjunction with Coordinated Defense and Segmentation. The more sensitive information would be stored in the deepest layers and enclaves of the system. To gain access those more sensitive enclaves should require greater privilege and in turn additional authentication. While this concept is inconsistent with the popular concept of single sign-on, it is very consistent with the underlying premise of resiliency – do not simply focus security (including authentication) at the perimeter.

Segmentation in some ways can impede Analytic Monitoring as the same boundaries that keep the adversary out, can block monitoring. To work effectively sensors need to be placed at various key points of the enclaves, and then the information from the various sensors need to be shared and coordinated to ensure a complete organization-wide perspective. Similarly, having IDSs and anti-malware capabilities at the various laptop, desktops and servers supports Coordinated Defense. But to fully support Analytic Monitoring the results of these sensor and tools must be combined to provide an organizational wide perspective.

Preparing for the Future

There are various technological, social and business trends that will have impact on the concept of access control. BYOD, cloud computing, the increased use of portable/mobile devices and Internet of Things all are to various degrees disrupting the traditional concept of security boundaries. All of these concepts erode the concept that an organization owns and controls the systems that process its critical information.

This in turn makes much more difficult for an organization to limit access to critical information and services. That said, in some ways these paradigm shifts lend themselves to some of the resiliency techniques. Separate devices are by default a form of segmentation. But if the devices are not designed with appropriate security protection in mind, then what was segmentation simply becomes ad-hoc placement of services and information, and that in turn is simply extending the attack surface.

Implicit in the concept of Coordinated Defense is the concept of coordination of the protections of the entities in question, and that there are defense mechanisms in place. The concept becomes far harder to enforce if the ownership and controls of the devices and other entities (e.g., appliances) becomes more disparate. With the advent of the Internet of Things the issue becomes even more complex as it becomes a challenge simply identifying the different entities that are remotely accessible and have an impact on the protection of information or services of an organization.

Analytic Monitoring is only as accurate and detailed as the data that feeds it. As organizational boundaries become more permeable data feeds must reflect and adapt to this permeability. This will include ensuring that an individual's identities can be tied to the specific individual to whom they belong regardless of the organization from which the information is coming.

In order to have effective access control in this brave new world one needs to:

1) Ensure that the various devices/entities each are designed with appropriate protections (Coordinated Defense); those that are not would either not be allowed access to the organization's infrastructure or only allowed via some encapsulated means that some virtualized thin client (Segmentation) might provide.

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

2) Have some means to identify all the devices/entities that have an impact on the security of the organization's mission. Devices not appropriately identified would be denied access. (Analytic Monitoring)
3) Restrict privileges for each device/entity only to that which they minimally require and to ensure that when devices employ a privilege that they are authorized to employ that privilege and apply it in the manner requested. Connections between devices may in some critical instances only be allowed if there were some trusted path, a bi-directional form of authentication, between the devices. (Privilege Restriction).

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