Secure Communication

Overview

A secure response infrastructure requires secure communications in order to keep cyber adversaries from inserting themselves into response and recovery processes when the usual communication mechanisms are compromised or otherwise unavailable. This document describes how to apply *Segmentation*[1]*, Substantiated Integrity,* and *Redundancy* resiliency techniques

Applying *Segmentation* to Limit Adversary Impacts

Segmentation – physical or logical separation or isolation of communications based on trustworthiness and criticality – can keep communications while withstanding and recovering from an attack from exposure to the adversary. 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:

- Logically isolate the security critical enclaves from ordinary enterprise operations.
    - 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.
- Protect and isolate communications related to incident response and recovery.
    - Use encryption (i.e., VPN) to provide protected, and logically isolated communications for security critical communications.

Applying *Substantiated Integrity* to Curtail Exposure to the Adversary

Substantiated Integrity – ascertaining whether critical services, information stores, information streams, and components have been corrupted – can prevent an adversary from delivering a payload, curtail the adversary's impact and enable an enterprise to recover from an attack more effectively. There are three approaches to *substantiated integrity*:

- Integrity Checks: Apply and validate checks of the integrity of information, components, or services.
- Provenance Tracking: Identify and track the provenance of data, software, and/or hardware elements.
- Behavior Validation: Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage).

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

Priorities for Immediate Action with *Substantiated Integrity*

- Require the use of cryptography to validate the authenticity of the sender.
  - Utilize certificates and digital signatures to validate the identity of the sender of communications (e.g., email, or SFTP).
- Use strong identification and authentication mechanisms to validate identity of senders and recipients of sensitive communications
  - Use strong authentication (e.g., multifactor authentication) to counter credential replay attacks.
  - Employ risk-based authentication where additional authentication is required for more privileged actions.
  - Implement periodic re-authentication of the communication path.
  - Use mutual authentication of both sender and receiver.

Applying *Redundancy* to Impede Adversary Actions

Redundancy – providing multiple protected instances of critical resources can curtail the time during which the adversary can impact mission functions and degrade the extent of that impact. There are three major implementation approaches to *redundancy*.

- Protected Backup and Restore: Back up information and software (including configuration data) in a way that protects its confidentiality, integrity, and authenticity, and to restore it in case of disruption or destruction.
- Surplus Capacity: Maintain extra capacity for information storage, processing, and/or communications that reasonably anticipates future needs.
- Replication: Duplicate information and/or functionality in multiple locations and keep it synchronized.

Priorities for Immediate Action with *Redundancy*

- Provide alternate or out-of-band communications methods for response staff.
  - These could involve secure bridges or Web portals in conjunction with a VPN to enable staff to access resources in the CSOC or CSIRT enclave.
  - Ensure that those who are involved in responding to cyber incidents have a means of communication (e.g., cell phone lists, satellite communications or paging system) that do not depend on the infrastructure that may be under attack (e.g., VOIP phones)
  - IPv4 and IPv6 are potential multiple communications path for the defenders as well as the adversary. IPv4 can be used as a redundant path if adequate safeguards have been taken in advance.

Preparing for the Future

Advanced adversaries will use the foothold they have already achieved in the organization's infrastructure in conjunction with stealth to compromise the organization's communication during recovery. In response, the organization needs to deceive the adversary using false communication paths, in order to force the adversary to prematurely reveal their presence and techniques. To limit targets of opportunity by the adversary, secure communications mechanism should be non-persistent in nature, and deployed when actually needed. Use *diversity* combined with *redundancy* and employ communication methods that are not used during normal operations (e.g., satellite communications), to avoid the chance of adversary compromise. Ideally, alternate secure communications mechanisms should be revealed only during critical post attack recovery times. This is done to limit the adversary's ability to detect the alternate mechanisms and develop appropriate means of attack. Tools for *substantiated integrity* are evolving to include approaches that will prevent man-in-the-middle and code injection type attacks.

Potential barriers to adoption of new techniques include the following:

- The cost of deploying alternate secure communications.
- The operational impact of training staff on alternate secure communications and the potential operational impact of having non-persistent secure communications (related to both the time required to initiate a new communications path and the impact on some environments where any delay could impede operations.)