Data Recovery Strategies

Overview

Responding to an adversarial attack requires protected data recovery processes and mechanisms in order to keep cyber adversaries from inserting themselves into response and recovery processes. This document describes how to apply *Adaptive Response*[1]*, Redundancy and Substantiated Integrity,* resiliency techniques.

Applying *Adaptive Response* to Limit Adversary Impacts

Adaptive Response – Implementing nimble cyber courses of action to manage risks – Optimizes an organization's ability to respond in a timely and appropriate manner to adversary activities, thus maximizing the ability to maintain the integrity and availability of core services. There are three approaches to applying *adaptive response*, the one most applicable to Data Recovery is*:*

- Dynamic Reconfiguration: Make changes to an element or component while it continues operating.

Priority for Immediate Action with *Adaptive Response*

- Use configuration management and dynamic reconfiguration tools to incorporate replacement applications and data.
    - Use configuration tools to track, control and manage changes to data and applications during the recovery process.
    - Use dynamic reconfiguration tools to swap in uncorrupted databases, and applications (e.g., gold copies hosted on a clean virtual system).
    - Identify and implement other solutions or products with much of the same data set to allow the organization to fight through.

Applying *Redundancy* to Limit 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.
- Replication: Duplicate information and/or functionality in multiple locations and keep it synchronized.

Priorities for Immediate Action with *Redundancy*

- Ensure that all tools and data involved in data recovery have backups.
    - Identify what tools and data are critical to data recovery.
    - Identify backups for these tools and data.
    - Test these backup resources (e.g., systems and tools) to ensure that the backups are adequate replacements for the main systems.
- Ensure that all individuals responsible for data recovery have adequately trained alternates that are available to implement data recovery procedures in the event the primary individuals are not available.

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

  - All individuals responsible (both primary and alternates) for data recovery should undergo the same training curriculum with regards to data recovery.
  - Adjust work and vacation schedules to make sure either the primary or the alternates are available as required.
  - As responsibilities shift reassess who is responsible for data recovery and train staff as appropriate.

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).

Priorities for Immediate Action with *Substantiated Integrity*

- Use the established system configuration baselines and the monitoring results to identify adversary presence in the resources used for data recovery.
  - Establish system configuration baselines for data and applications whenever a system is modified.
  - Identify mechanisms to compare the baselines with monitoring data.
- Verify the identity of an individual during the data recovery process before using information, direction or tools the individual has provided.
  - Establish processes for identifying individuals using both in-band and out-of-band procedures that are not vulnerable to the same types of attack.
  - Establish and update the list of authorized individuals who will be providing information, direction and tools during a time when data recovery processes are implemented.

Preparing for the Future

As cloud computing and embedded systems are integrated into the environment, the manner in which data recovery is performed must adapt. With cloud computing, administrators cannot physically touch the systems being restored. This removes some options (e.g. a CD with a gold copy) of data recover. On the other hand, an instance of the software or data in the cloud can be the backup resource used in the data recovery process. Embedded systems provide a challenge to data recovery due to rigid, sometimes misunderstood, interfaces. As the number of embedded systems in the environment increases, it becomes more critical to identify these systems and ensure that the interfaces are understood and taken into account when preparing for data recovery. Incorporating *Diversity* into *Redundancy* will bring strength to the redundant systems and data, enabling them to better withstand an attack and be available for recovery. In addition, adding cryptographic checksums to the data will enable defenders to identify corrupted malware more easily before it is used to restore a system. This will improve the defenders ability to remove the adversary from their systems.