Backup Strategies

Overview

The design principles for backup strategies enable resilience-enhancing technical processes, and integrate them into existing and new infrastructure services, to expand resiliency from disaster recovery to cyber resiliency in a cost effective way. This document describes how to apply *segmentation*, *redundancy* and *substantiated integrity*[1] resiliency techniques to an organizations backup strategy. Backup Strategies rely on appropriately implemented access control as well. This topic is addressed in the Access Control Guide.

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. Separation or isolation can be physical or logical, and predefined or dynamic. The backup strategy should plan for segmentation of backup data and systems.

- 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 backups from primary systems.
  - Use logical (e.g., virtualization) or physical separation (e.g., air gaps) to maintain a protected backup
  - Consider using an alternate processing facility.
- Logically and physically separate components based on degree of trust in system management and security.
  - Keep backups from systems with a high level of trust separate from those with a lower level of trust using stronger means of separation (e.g., physically separate such segments).
- Replicate key functions and ensure segments are self-sufficient.
  - Employ some form of dependency/criticality analysis to identify key functions; once they are identified, ensure that they are replicated.
  - Perform tests (e.g., live tests, tabletop exercises) to determine whether key functions are replicated and segments are self-sufficient.

Applying *Redundancy* to Degrade the Adversary's Impact

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*.

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

- 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. The surplus should anticipate reasonable future needs
- Replication: Duplicate information and/or functionality in multiple locations and keep it synchronized.

Priorities for Immediate Action with *Redundancy*

The top priorities for *Redundancy* are:

- Create and maintain protected copies of critical information.
    - Check critical information to make sure that it is complete.
    - Test protections on critical information to ensure that the redundant copies do not provide inappropriate access.
- Test failover systems to ensure proper operation.
    - Perform tests to ensure enough capacity is available for backup services to take on the critical functions they are replacing.
    - Perform tests to ensure critical personnel have the access they need. This may be different from the access individuals would normally have due to the fact that the backup services would be put in place when the enterprise is under attack.

Applying *Substantiated Integrity* to Recover from Adversary Actions

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/Quality Checks: Apply and validate checks of the integrity or quality 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*

- Test backup systems on a frequent basis and ensure the data is properly backed up.
    - Use tamper-evident technologies, checksums and other tools (e.g., code-canaray type technology) to ensure the adversary has not tampered with backups in preparation for a future attack.
    - Use automated testing frameworks to test that backups systems will work as required.
- Use an approved data integrity-verification technique in conjunction with data backups as an indicator of data corruption.
    - Before restoring data, check to make sure it conforms to the specified requirements and is internally consistent across all backups.
    - When restoring from backups, employ non-repudiation tools such as cryptographic certificates and signatures to ensure data and services can be trusted.

Preparing for the Future

The technological trend towards the increased use of portable/mobile devices and the internet-of-things disrupts the traditional concept of security boundaries. While this can provide some redundancy – data might be backed up on a mobile device, it also provides hidden connectivity that may violate the assumptions of a segmented environment.

As deception techniques improve, hiding backup data and services while providing a honeynet that looks like the real backup network, can become an effective means of keeping the adversary unaware of these resources. This can speed recovery as the organization is not fighting to protect both the main systems and data at the same time it is trying to protect the backup resources.

With increasing interface standards, another way to degrade attacks on backup systems and services is to increase diversity. That way an attack works on one type of system or service, it may fail on the other types and therefore leave the enterprise with some backup services. If, in addition, portable or otherwise geographically disparate redundant assets and functionality are maintained, the organization can protect itself from an attack focused at a specific location as well.