Architect to Protect

Overview

The design principles for architectural foundations enable resilience-enhancing technologies to be integrated with security and other infrastructure services in a cost effective way. This document describes how to apply *segmentation*, *coordinated defense* and *diversity*[1] resiliency techniques.

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.

- 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

- Apply *segmentation* to enterprise capabilities for cyber defense and recovery. These have the advantage of being less subject to the current trends toward integration, convergence, and "moving everything to the cloud."
    - 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 related to incident response and recovery. Preferably, use a VPN, but at a minimum encrypt messages between staff involved in response and recovery.
    - Use logical or physical separation to maintain a protected backup or alternate processing facility.
- 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.

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

- Perform penetration testing or use a red team to determine whether the apparent separation is real. This testing should also determine the implications for protected enclaves if shared services are compromised.

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. 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 are defined and implemented consistently across component systems and networks,
  - Jointly define *Cyber Courses of Action* and
  - Ensure useful placement of cyber sensors.
- Analyze changes (e.g., addition of capabilities, changes in configuration, software updates, hardware refreshes) to component systems and network segments to ensure that interoperability is preserved, and that a disruption (e.g., attack, accident) that involves one defensive mechanism or one component system or network segment does not negate, degrade, or destabilize another.
- Manage how component systems and network segments use defensive mechanisms (e.g., making configuration changes, turning on some mechanisms while turning off others, deciding when and how to update or patch software) based on changes in the operational environment, while maintaining consistency.
  - Provide equivalent security capabilities at different architectural layers.
  - Employ a systematic process to identify dependencies and interactions among cyber defenses, security controls, and performance controls.

Applying *Diversity* to Impede Adversary Actions

Diversity - using a heterogeneous set of technologies (e.g., hardware, software, firmware, protocols) and data sources – can minimize the impact of attacks and force adversaries to attack multiple different types of technologies. There are several synergistic implementation approaches to diversity:

- Architectural Diversity: Use multiple sets of technical standards, different technologies, and different architectural patterns.
- Design Diversity: Use different designs to meet the same requirements or provide equivalent functionality.
- Synthetic Diversity: Transform implementations to produce a variety of instances, so that for no specific instance is the implementation completely predictable.
- Information Diversity: Provide information from different sources or transform information in different ways.
- Command, Control, and Communications (C3) Path Diversity: Provide multiple paths, with demonstrable degrees of independence, for information to flow between elements.

- Supply Chain Diversity: Use multiple, demonstrably independent, supply chains for critical components.

Priorities for Immediate Action with *Diversity*

- Recognizing that some diversity will always be present in an enterprise architecture, leverage these technologies (e.g., different browsers on operating systems, diversity of apps on smartphones and tablets, different antivirus and antimalware products) but ensure that security controls are consistent across the diverse technologies.
- Increase diversity by using different protocols / communications diversity (e.g., over time, space, frequency), by supporting different platform suites for end users (e.g., some using tablets, some laptops) and providing diverse mechanisms for critical security services, e.g., authentication.
- Investigate the possibility, and evaluate the cost-benefit tradeoffs, of using different suppliers of critical components in the supply chain.

Preparing for the Future

Segmentation, like business continuity planning, relies on an understanding of how mission or business processes rely on cyber resources, and on the functional dependencies among those resources. That understanding enables an organization to determine the relative criticality of its resources, and thus to define an enterprise architecture in which physical or virtual enclaves are – or can be – separated based on the importance of defending them. However, mission or business processes evolve over time, and thus so do dependencies. Therefore, enterprise architects and systems engineers need to maintain an ongoing dialog with mission or business process owners.

Similarly, *coordinated defense* relies on the 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.

Diversity can increase due to non-resiliency business and mission pressures as well as an effort to increase resiliency. Resilient diversity can leverage this business related diversity but should not be limited to this. Understanding the organization's diversity and maintaining an accurate representation is key to managing the enterprise security consistently.

A growing chorus of experts recommend making conscious risk management decisions that include resilience and defensibility, recognizing that such recommendations run counter to the trends toward integration, convergence, and cloud computing. Enterprise architects and systems engineers should be prepared for a pendulum swing, in which they are asked whether and how they have managed risks of malware permeating the enterprise information infrastructure. These resiliency techniques are primary strategies for limiting the spread of malware, detecting it early and recovering from the attack quickly.

Further Reading & References

- Richard J. Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*, at http://www.cnas.org/sites/default/files/publications-pdf/CNAS_PoisonedFruit_Danzig_0.pdf
- Dan Geer, "Cybersecurity as Realpolitik," BlackHat Keynote Address, at http://geer.tinho.net/geer.blackhat.6viii14.txt

- Carson Zimmerman, *Ten Strategies of a World-Class Cybersecurity Operations Center*, at http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf