Segregating Networks and Functions

After gaining initial access to a network, adversaries traverse the allowed communication paths between network devices to gain deeper access. However, a securely segregated network can greatly reduce an adversary's ability to access sensitive portions of the network.

Why are Network and Function Segregation Important?

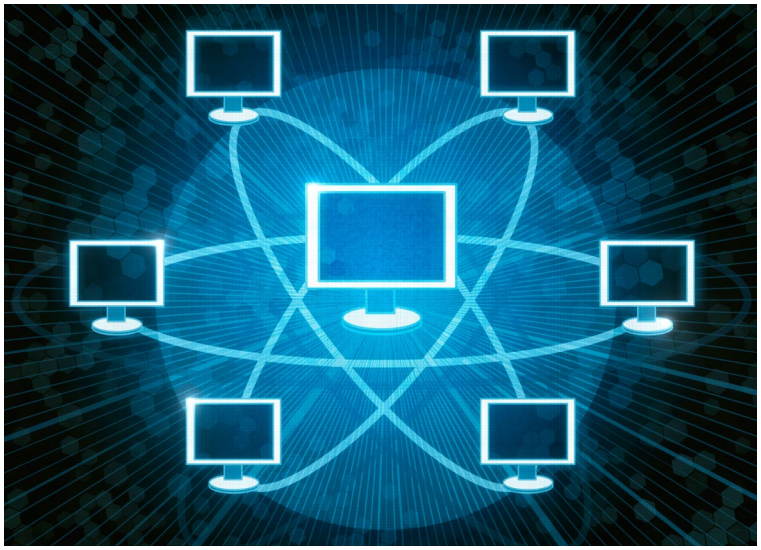
Networks are composed of interconnected devices with varying functions, purposes, and sensitivity levels. Networks can consist of multiple segments that may include web servers, database servers, development environments, and the infrastructure that binds them together. Because these segments have different purposes as well as different security concerns, segregating them appropriately is paramount in securing a network from exploitation and malicious intent.

If an adversary is able to acquire access and the network is not properly segregated, he will be able to expand his access and move freely throughout the network. When networks are segregated into smaller portions with communications restricted between segments, an adversary's access is limited in scope, and the ability to traverse the network is severely restricted.

Hampering an intruder's ability to gain further access in a network is vital to protect sensitive information and allows for easier remediation upon discovery. Limiting device communication enables better monitoring and easier discovery of intruder attempts to spread from one area to another.

Recommended Mitigations

Properly segregated networks contain completely separate infrastructure for each functional area within an organization. This includes providing separate servers, storage devices, routers, and switches for different areas of varying sensitivity and access. For example, devices involved with financial transactions should be fully separated both logically and physically from those devices that serve the purpose of public web access. The following are recommendations for segregating networks and their functions.



Physically Segregate Network Segments Whenever Possible

Providing an independent infrastructure for each major function in the network can limit an intruder's ability to move with ease across network devices. Sensitive functions (such as financial transactions) should have an infrastructure that is physically separate from the remote or publicly accessible web environment.

Logically Segregate Network Segments by Using Private VLANS

Do not rely on traditional virtual local area networks (VLANs) as a security control, as these can be circumvented. Instead, use private VLANs with port restriction. Unlike VLANs, private VLANs prevent hosts on the same subnet from communicating with other hosts on the same subnet. This type of VLAN can secure sensitive organizational functions such as accounting, human resources, payroll or intellectual property. Devices within a private VLAN are only permitted to communicate within their trusted network environment.

Protect Sensitive Accounts in Segregated Networks and Organizational Functions

Preventing a malicious actor from exploiting credentials and gaining unauthorized access to administrative or executive accounts is vital to protecting information. Limiting these privileged accounts and credentials can further deny unauthorized access. Pass-the-Hash (PtH) is a commonly used technique used to elevate privileges or gain access to sensitive information. Many of the recommendations associated with PtH can assist with restricting adversarial movement or access.

Additional Information

- Control Administrative Privileges
  http://www.nsa.gov/ia/mitigation_guidance/
- Limiting Workstation to Workstation Communication
  http://www.nsa.gov/ia/mitigation_guidance/
- Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques
  http://www.microsoft.com/en-us/download/details.aspx?id=36036
- Reducing the Effectiveness of Pass-the-Hash
  http://www.nsa.gov/ia/_files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf
- Securing Networks with Private VLANs and VLAN Access Control Lists
  http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a008013565f.shtml
- Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines
  http://www.sans.org/critical-security-controls/

Contact Information

Industry Inquiries: 410-854-6091

USG/IC Client Advocates: 410-854-4790

DoD/Military/COCOM Client Advocates: 410-854-4200

General Inquiries: **niasc@nsa.gov**