Network Mitigations Package-Infrastructure (NMP-I)

June 2016

The Increasing Threat to Network Infrastructure Devices

The advancing capabilities of organized hacker groups and nation state cyber adversaries create an increasing global threat to information systems. The rising threat levels place more demands on security personnel and network administrators to protect information systems. Due to increased workloads, security professionals often overlook network infrastructure security. Protecting the network infrastructure is critical to preserve the confidentiality, integrity, and availability of communication and services across an enterprise. If the network infrastructure is compromised, malicious hackers or adversaries can gain full control of the network infrastructure allowing traffic to be redirected, changed, or denied. Intruders with infrastructure privilege and access can impede productivity and severely hinder re-establishing network connectivity. Networks are vulnerable, the cyber threat is real, and in this current state there has never been a greater need to improve network infrastructure security.

Network infrastructure consists of interconnected devices designed to transport communications needed for data, applications, services, and multi-media. Perimeter devices such as firewalls and intrusion detection systems have been the traditional methods used to secure the network, but as threats change, so must our security strategies. Organizations can no longer rely on perimeter devices to protect the network from cyber intrusions; we must also be able to contain the impact/losses within the internal network and infrastructure.

Network Infrastructure Mitigations Overview

The security community continues to address emerging network threats. The new security model now consists of prevention, detection, containment, and response to mitigate threats. The Network Mitigations Package-Infrastructure (NMP-I) focuses on layering information system network defenses enabling communications while controlling adversaries' ability to move laterally through the network. The NMP-I provides guidance to aid organizations as well as system administrators in hardening core network infrastructure to protect network infrastructure access, network availability, and critical information.

The NMP-I recommends the following:

- Segregate networks and functions
- Limit unnecessary lateral communications
- Harden network devices
- Secure access to infrastructure devices
- Perform Out-of-Band network management
- Validate integrity of hardware and software

Segregate Networks and Functions

Proper network segmentation is a very effective security mechanism to prevent an intruder from propagating exploits or laterally moving around an internal network. On a poorly segmented network, intruders are able to extend their impact to control critical devices or gain access to sensitive data and intellectual property. Security architects must consider the overall infrastructure layout, segmentation, and segregation. Segregation separates network segments based on role and functionality. A securely segregated network can contain malicious occurrences, reducing the impact from intruders, in the event that they have gained a foothold somewhere inside the network.

Physical Separation of Sensitive Information

Local Area Network (LAN) segments are separated by traditional network devices such as a router. Routers are placed between networks to create boundaries, increase the number of broadcast domains, and effectively filter users' broadcast traffic. These boundaries can be used to contain security breaches by restricting traffic to separate segments and can even shut down segments of the network during an intrusion, restricting adversary access.

Recommendations:

- Implement Principles of Least Privilege and need-to-know when designing network segments

MFS U/OO/801549-16

- Separate sensitive information and security requirements into network segments
- Apply security recommendations and secure configurations to all network segments and network layers

Virtual Separation of Sensitive Information

As technologies change, new strategies are developed to improve IT efficiencies and network security controls. Virtual separation is the logical isolation of networks on the same physical network. The same physical segmentation design principles apply to virtual segmentation but no additional hardware is required. Existing technologies can be used to prevent an intruder from breaching other internal network segments.

Recommendations:

- Use Private Virtual LANs to isolate a user from the rest of the broadcast domains
- Use Virtual Routing and Forwarding (VRF) technology to segment network traffic over multiple routing tables simultaneously on a single router
- Use Virtual Private Networks (VPNs) to securely extend a host/network by tunneling through public or private networks

Limit Unnecessary Lateral Communications

Allowing unfiltered workstation-to-workstation communications (as well as other peer-to-peer communications) creates serious vulnerabilities, and can allow a network intruder to easily spread to multiple systems. An intruder can establish an effective "beach head" within the network, and then spread to create backdoors into the network to maintain persistence and make it difficult for defenders to contain and eradicate.

Recommendations:

- Restrict communications using host-based firewall rules to deny the flow of packets from other hosts in the network. The firewall rules can be created to filter on a host device, user, program, or IP address to limit access from services and systems.
- Implement a VLAN Access Control List (VACL), a filter that controls access to/from VLANs. VACL filters should be created to deny packets the ability to flow to other VLANs.
- Logically segregate the network using physical or virtual separation allowing network administrators to isolate critical devices onto network segments.

Harden Network Devices

A fundamental way to enhance network infrastructure security is to safeguard networking devices with secure configurations. Government agencies, organizations, and vendors supply a wide range of resources to administrators on how to harden network devices. These resources include DISA STIGs, NSA guides, benchmarks, and best practices. These recommendations should be implemented in conjunction with laws, regulations, site security policies, standards, and industry best practices. These guides provide a baseline security configuration for the enterprise that protects the integrity of network infrastructure devices. The NMP-I supplements the network security best practices supplied by vendors.

Recommendations:

- Disable unencrypted remote admin protocols used to manage network infrastructure (e.g. Telnet, FTP, etc)
- Disable unnecessary services (e.g. discovery protocols, source routing, HTTP, SNMP, BOOTP)
- Use SNMPv3 (or subsequent version) but do not use SNMP community strings
- Secure access to the console, auxiliary, and VTY lines
- Implement robust password policies and use the strongest password encryption available
- Protect router/switch by controlling access lists for remote administration
- Restrict physical access to routers/switches
- Backup configurations and store offline
- Use the latest version of the network device operating system and update with all patches
- Periodically test security configurations against security requirements

- Protect configuration files with encryption and/or access controls when sending them electronically and when they are stored and backed up

Secure Access to Infrastructure Devices

Administrative privileges on infrastructure devices allow access to resources that are normally unavailable to most users and permit the execution of actions that would otherwise be restricted. When administrator privileges are improperly authorized, granted widely, and/or not closely audited, intruders are able to exploit them. These compromised privileges can enable adversaries to traverse a network, expanding access and potentially allowing full control of the infrastructure backbone. Unauthorized infrastructure access can be mitigated by properly implementing secure access policies and procedures.

Recommendations:

- **Implement Multi-Factor Authentication**
  Authentication is a process to validate a user's identity. Weak authentication processes are commonly exploited by attackers. Multi-factor authentication uses at least two identity components to authenticate a user's identity. Identity components include something the user knows (i.e. password), an object the user has possession of (i.e. token), and a trait unique to the specific person (i.e. biometric).
- **Manage Privileged Access**
  Use an authorization server to store access information for network device management. This type of server will enable network administrators to assign different privilege levels to users based on the Principle of Least Privilege. When a user tries to execute an unauthorized command, it will be rejected. To increase the strength and robustness of user authentication, implement a hard token authentication server in addition to the AAA server, if possible. Multi-factor authentication increases the difficulty for intruders to steal and reuse credentials to gain access to network devices.
- **Manage Administrative Credentials**
  Although multi-factor authentication is highly recommended and a best practice required by DoDI 8520 for DoD, systems that cannot meet this requirement can at least improve their security level by changing default passwords and enforcing complex password policies. Network accounts must contain complex passwords of at least 14 characters from multiple character domains including lowercase, uppercase, numbers, and special characters. Enforce password expiration and reuse policies. If passwords are stored for emergency access, keep these in a protected off-network location, such as a safe.

Perform Out-of-Band Management

Out-of-Band (OoB) management uses alternate communication paths to remotely manage network infrastructure devices. These dedicated paths can vary in configuration to include anything from virtual tunneling to physical separation. Using OoB access to manage the network infrastructure will strengthen security by limiting access and separating user traffic from network management traffic. OoB management provides security monitoring and can implement corrective actions without allowing the adversary who may have already compromised a portion of the network to observe these changes.

OoB Management can be implemented physically or virtually, or through a hybrid of the two. Building additional physical network infrastructure is the most secure option for the network managers, although it can be very expensive to implement and maintain. Virtual implementation is less costly, but still requires significant configuration changes and administration. In some situations, such as access to remote locations, virtual encrypted tunnels may be the only viable option.

Recommendations:

- Segregate standard network traffic from management traffic
- Enforce that management traffic on devices only comes from the OoB
- Apply encryption to all management channels
- Encrypt all remote access to infrastructure devices such as terminal or dial-in servers
- Manage all administrative functions from a dedicated host (fully patched) over a secure channel, preferably on the OoB

- Harden network management devices by testing patches, turning off unnecessary services on routers and switches, and enforcing strong password policies
- Monitor the network and review logs
- Implement access controls that only permit required administrative or management services (SNMP, NTP SSH, FTP, TFTP)

Validate Integrity of Hardware and Software

Products purchased through unauthorized channels are often known as "counterfeit," "secondary," or "grey market" devices. There have been numerous reports in the press regarding grey market hardware and software being introduced into the marketplace. Grey market products have not been thoroughly tested to meet quality standards and can introduce risks to the network. Lack of awareness or validation of the legitimacy of hardware and software presents a serious risk to users' information and the overall integrity of the network environment. Products purchased from the secondary market run the risk of having the supply chain breached, which can result in the introduction of counterfeit, stolen, or second-hand devices. This could impact network performance and may compromise the confidentiality, integrity, or availability of network assets. Furthermore, breaches in the supply chain provide an opportunity for malicious software or hardware to be installed on the equipment.

Recommendations:

- Maintain strict control of the supply chain; purchase only from authorized resellers
- Require resellers to implement a supply chain integrity check to validate hardware and software authenticity
- Inspect the device for signs of tampering
- Validate serial numbers from multiple sources
- Download software, updates, patches, and upgrades from validated sources
- Perform hash verification and compare values against the vendor's database to detect unauthorized modification to the firmware
- Monitor and log devices, verifying network configurations of devices on a regular schedule
- Train network owners, administrators, and procurement personnel to increase awareness of grey market devices

Contact Information

Industry Inquiries:
Business Affairs Office
410-854-6091
email: bao@nsa.gov

Client Requirements and General Information Assurance Inquiries:
IAD Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov

Disclaimer: The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

