NATIONAL SECURITY AGENCY
CYBERSECURITY INFORMATION

ACTIVELY MANAGE SYSTEMS AND CONFIGURATIONS

CHANGE IS A CONSTANT

Networks are often complex, and in a constant state of change. Devices are connected and removed. Software is updated. Attackers can use knowledge of network systems and configurations to compromise them. Without a clear picture of network status, mitigating cyber threats becomes difficult. In a world of ever-escalating threats, it is critical to ensure visibility into the systems and configurations of enterprise networks.

Active management of these systems and configurations is vital to a network's security posture. It provides visibility and enables decisive defensive action. Other critical mitigations directly depend on active management, such as hunting for intrusions and exercising a system recovery plan. Enterprises that actively manage their networks also save resources and improve their network availability [1].

To achieve this, an enterprise first discovers and inventories all systems on the network. Next, the enterprise establishes the ability to manage the configuration of systems on the network. Finally, the enterprise engages in continuous and dynamic management of systems in the face of ever-evolving threats.

DISCOVER AND INVENTORY NETWORK SYSTEMS

Before systems can be managed, they must be identified. Surveys discover and document the location of wired systems such as servers, desktops, and network devices including routers, switches, and unified communications devices.

Network discovery and mapping tools can help supplement this information by locating any unknown systems and also discovering wireless devices or any new systems that appear unexpectedly on the network. Administrators can then remove any such systems that are unwanted, unneeded, or unexpected. Port Security and Network Access Control technologies can also be used to limit or discover any unexpected systems, although there is overhead in these approaches and they may not be appropriate for all networks.

Once the system inventory is documented, administrators should establish a process to update the inventory as needed based on changes in the network. This ensures the inventory remains current. The inventory should minimally capture the physical location, owner, and purpose of the device. Some parts of networks cannot be effectively inventoried, such as those that support guest devices like mobile devices. These network segments should be segregated from the rest of the network and enterprise resources.

MANAGE CONFIGURATION

After all systems are identified, administrators can manage their configurations. Managing the configuration of systems provides administrators visibility and control over ongoing network operations and ensures changes can be made when needed. Systems management tools not only provide the ability to manage configurations, but also to query other important aspects of the system, such as determining currently installed software. Enterprises can choose from a variety of commercially-available offerings to achieve management of systems.

Traditionally, configuration management solutions only offered the ability to control servers and workstations. Now, many IT endpoints are mobile devices [2]. Alternative Mobile Device Management (MDM) solutions exist, supporting the management of mobile devices that connect to and process enterprise data. Because of their mobile nature, these devices do not have a consistent location and instead their physical protection is the responsibility of the primary user. MDM-style management is also available for desktop and laptop platforms that serve a single user or handful of users. While this approach does not provide the single sign-on capability an integrated directory system provides, it does separate authentication and management in a way that eliminates some risks inherent in single sign-on architectures.

At first, managing security configurations began with a focus on one-time hardening of settings to reduce the attack surface. Over the last 20 years, the industry has largely transitioned from shipping enterprise-class products with permissive and vulnerable configurations to shipping products whose configurations are largely secure by default. Yet managing security-relevant settings still constitutes due diligence, and a small number of settings have significant preventive cybersecurity impact. These include enabling automatic software updates, disabling removable media access if the operational environment permits, and enforcing software execution policies.[1] Industry often provides configuration checklists for popular products, and enterprises can adopt these with confidence that they will track with the products and introduce little to no overhead.

A configuration control process must also be established to manage the enterprise's configuration for each type of system. Network stakeholders supported by Subject Matter Experts should be involved in decision-making regarding configurations and play an essential role in the enterprise's configuration management plan. At the same time, this process must be agile and establish contingencies to make decisions within minutes if operationally needed.

MONITOR AND MANAGE SYSTEMS AND SOFTWARE

To quickly respond to any threats, administrators must continue to monitor systems and software on the network, and promptly take action when needed. Continuous management allows cybersecurity and IT operation teams to truly control the network and contest adversary actions.

Effective monitoring and management includes continuous discovery of new systems, vulnerability assessments, management of configurations, immediate patching, and analytics that leverage security information and event management services. Implementation of continuous monitoring enables a real-time view of the current state of the network, even as configurations change and devices connect to and disconnect from the network. The real-time view established by continuous monitoring can then inform everyday management of servers, workstations, and network devices. This ensures all systems are in the intended state. The ability to access current information about all systems on the network, as well as historical information, is also critical to effective incident response.

CONCLUSION

Networks continue to grow in complexity, as does the risk from adversaries. Establishing control of the network lays the groundwork for countering adversary behavior as well as implementing proactive network defense. To actively manage its networks, an enterprise regularly inventories its systems, evaluates configurations, tracks changes, monitors behaviors, and conducts regular assessments, assuring its understanding of the network is current and comprehensive. This approach results in reduced costs for the enterprise, increased network availability, and better preparedness against network attacks.

REFERENCES

[1] "Configuration Management: Best Practices White Paper," Cisco, Doc. ID 15111, 2006. [Online] Available: https://www.cisco.com/c/en/us/support/docs/availability/high-availability/15111-configmgmt.html

[2] "What Is Mobile Device Security?" Cisco. [Online] Available: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/mobile-device-security.html

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

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.

CONTACT INFORMATION

Client Requirements and General Cybersecurity Inquiries
Cybersecurity Requirements Center (CRC), 410-854-4200, email: Cybersecurity_Requests@nsa.gov

[1] For more information on these settings, please refer to "Enforce Signed Software Execution Policies" and "Update and Upgrade Software Immediately," part of the *NSA Cybersecurity Top 10 Mitigations.*