Information Security in Large-Scale Practice

Brooks B. Chamberlin
chamberlinb@hq.5sigcmd.army.mil

Information Assurance Program Manager
United States Army, Europe
Mannheim, Germany

Abstract

The United States Army, Europe's (USAREUR's) wide area network (WAN) for sensitive but unclassified information contains approximately 50,000 information systems in 2,000 local area networks (LAN). Since the mid-1990's, USAREUR has incrementally implemented policies, technical tools, and security training to defend that WAN against various cyber threats. The sheer size of this WAN and the requirement that it afford users access to the Internet constitute significant security challenges.

On this scale, network defense must be accomplished in depth, with each layer restricting the scope of permitted network activity to the minimum needed. Varying requirements for connectivity and the coarse selectivity of available network-level security tools limit the network perimeter defenses to the lowest common denominator. Therefore, local units must apply access controls and firewalls that are tailored to their needs. Then the security configuration of individual servers and systems must be managed closely, and regular scans to identify vulnerabilities and viruses run.

Policies and training for key information technology personnel are the essential first step to applying defense in depth across a large organization. However the organization's culture and the available resources must be addressed for change to have measurable effect. Network security functions must shift from their traditional separate staff chain and be embedded in network operations: decisions on what and how to defend directly affect how the network will operate. Similarly, configuration of operating systems and applications at the LAN level must be managed together with security configuration. Dedicated security resources are needed locally to help units apply available defensive tools and major subsets of the WAN should be managed on a regional basis to allow dynamic adjustments that consider the needs of the using military unit.

Keywords: network defense, network security, WAN.

1. Introduction

The United States Army, Europe (USAREUR) operates multiple wide area networks (WAN). The WAN used for sensitive but unclassified (SBU) information presents some of our greatest security challenges due to its size and the need for many of its users to access the Internet. This WAN contains approximately 50,000 information systems in 2,000 local area networks (LAN) across parts of Germany, Italy, Belgium, the Netherlands, the United Kingdom, and in the Balkans. Since the mid-1990's, USAREUR has incrementally implemented policies, technical tools, and security training to defend that WAN against hackers, viruses, and other cyber threats.

While USAREUR's SBU WAN is a single entity, subordinate organizations usually own and operate their own servers and control the structure and configuration of their own LAN. This autonomy makes the LAN responsive to each unit's needs, but presents challenges in ensuring that common security standards are adhered to.

Connection of this WAN to the Internet is necessary for conduct of official business, primarily logistics, contracting, and research. Internet access is also permitted for activities related to morale. In the final analysis, decisions regarding permitted activities, network configuration, security, and operation are made on a three-way balance of operational efficiency, security, and morale. We are constantly seeking solutions that can increase security while not reducing our ability to accomplish all missions and protecting morale-related services.

2. Current Defenses

The present network defenses can be equated to 'walking' on the scale of 'crawl, walk, run.'

These defenses span from technical tools to policy and training. Due to the environment introduced above, they must be applied in layers. Defensive restrictions imposed at the network perimeter are limited to the lowest common denominator of requirements across the entire WAN. Regions, military communities, or organizations can apply more stringent controls tailored to their local requirements. Finally, individual servers and workstations must be configured to further reduce exposure to risk.

2.1 Policy and Program

To provide for common standards across all organizations connected to the WAN, policies have been incrementally developed and published by USAREUR. These include guidance on the form and life span of passwords, updating anti-virus, required security training for users and systems administrators, prohibited on-line activities and behavior, compliance with configuration baselines, and other minimum standards. The policies are developed and approved through an Information Assurance (IA) Council of Colonels.

The basic program also includes issuance of Information Assurance Vulnerability Alerts (IAVA) that warn of identified vulnerabilities in software. IAVA provide mandatory actions that will reduce the risk of their exploitation by hackers.

The program also mandates a test for all computer users before they may receive a log-on and password in the network. It also mandates two-to-four weeks of classroom and hands-on computer network security training for all system administrators and network managers. These classes are offered at no cost to USAREUR units at 12 locations across the theater.

2.2 Network Perimeter

The perimeter of the WAN consists of gateways into the greater Department of Defense WAN, and further to the Internet. At these gateways, access controls on border routers are used to block selected ranges or domains of Internet Protocol (IP) addresses and ports associated with known hacker tools or not needed for authorized network services. Activity passing through these routers is then monitored by intrusion detection systems (IDS) that identify patterns of activity that could be hostile to the network. Logs of router activity and the IDS events are triaged by our Regional Computer Emergency Response Team (RCERT) to detect intrusions or incidents. When that team identifies dangerous or illegal activity, it works with the affected unit, criminal investigators, and counter-intelligence services to contain damage and investigate the incident.

2.3 Community or Organization Level

Below the network perimeter, organizations can apply more restrictive access controls, secure protocols, and firewalls, or use virtual private networks to manage access to their campus area network (CAN) or LAN. Software for these tools is provided at no charge by the RCERT, along with training and assistance in configuring and installing these security measures. Units must decide how they want to tailor application of these tools to meet their organization's needs.

The RCERT also develops and provides detailed baselines of secure configuration settings for units to apply to their servers and workstations. The IA Program Manger's staff then helps units to accredit their systems and networks and to check their compliance with both the secure baselines and IAVA. Units can either sign out scanning tools and check their local network for vulnerabilities or ask for the RCERT to perform such scans for them.

Finally, individual organizations carry out the security policies established by USAREUR. They ensure that users and systems administrators attend training, they change passwords and update anti-virus software, and they configure systems securely.

2.4 Challenges

Experience in implementing the current defenses have identified challenges and shortcomings that we must address to bring our network protection up to the ‘run’ level on the ‘crawl, walk, run’ scale.

Because most organizations control their own servers and system administrators, and because compliance with security baselines for system configurations is hard to maintain, actual compliance of system configurations is inconsistent.

The RCERT cannot keep up with all requests for assistance to install firewalls, run vulnerability scans, and apply other technical tools. Further, many units have not proactively pursued application of such improvements to their networks.

More refined security tools are needed to further reduce our exposure to cyber threats and to reduce risk while still permitting all required network activity.

Finally, as network use continues to expand exponentially, centralized intrusion detection and reaction will not be able to adequately keep up with the threat and with varying security needs and priorities of the many warfighting organizations using the WAN.

3. Road Ahead

In light of the challenges identified above, we have developed a series of azimuths for improvement of network security.

3.1 Simplified Configuration Compliance

We must make compliance with secure configuration standards easier to do. Quick ways to identify all pertinent vulnerabilities and associated fixes for each system and application are essential. Then software tools are needed to speed the process of applying these fixes and to check results. We are working now on simplified step-by-step secure baselines, matrices of vulnerabilities and fixes for different operating systems and applications, and an automated tool to identify, apply, and check all configuration security elements.

3.2 Regional Network Operations

Full time, trained network security specialists are needed on a local level to encourage units and help them implement defense in depth measures. We are adding network security specialists to many of our 30 local Network Service Centers (NSC) to help units scan their systems for vulnerabilities, install firewalls, establish virtual private networks, and take other security steps. The NSC will focus on LAN level issues.

We are also establishing six regional Network Operations & Security Centers (NOSC). These NOSC will be aligned with major warfighting organizations and be responsible for both network management and network security at the CAN level. They will have visibility across the CAN, including perimeter network defenses in their region, host-based IDS, and the configuration of systems in LAN connected to the CAN.

Both of these organizations will tightly link network operations and management with network security. Instead of being worked in a security stovepipe, security decisions will be made in tandem with operational decisions and will be in tune with the priorities of the unit Commander in that region. The NOSC and NSC will be able to use their network visibility and close interaction with local systems administrators to improve and enforce compliance with security standards.

An eventual development of these regional operations may be the consolidation of all servers under the NSC and NOSC. Units will be reluctant to give up their ownership and control of these systems, but consolidation would offer resource efficiencies and much simpler management of both operational and security configurations.

4. Conclusions

If security is made too hard to comply with and is not fully resourced, obviously it will not be done. Although network security is a new field and resources have not always been provided for it, we must make it a priority and make it simple to accomplish.

Security must be fully integrated into the realm of network operators rather than remain separate. Dynamic events will call for responsive security decisions and changing security measures. Further, network management activities directly impact on network security. We can more effectively meet our security needs if they are understood and embedded in network operations.