Security, Government & Infrastructure

Life Cycle Information Assurance

Online Data Reveals Computer Security Threats

With increasing intrusions of government computer networks, information assurance (IA) has become a vital issue, especially for the nation's leading weapon developers. The U.S. Army Aviation and Missile Command (AMCOM) at Redstone Arsenal, Alabama, is the military's leading research and development center responsible for weapon systems such as the Blackhawk and Apache helicopters and the Patriot Missile system. To make information readily accessible for logistics and other functions, AMCOM employs numerous client/server and Web-based systems, requiring storage of tremendous amounts of data on Internet-accessible file and Web servers. With more data online, internal and external anomalies, malicious hackers, and other security issues have become an increasing concern. AMCOM needed to take proactive steps to secure the Army's assets in a way that allowed continued access to critical operational and programmatic data.

The Project Objectives:

- Secure the Army's online data assets
- Ensure continued data accessibility for critical operational and programmatic data

The Solution:

After a network assessment revealed certain vulnerabilities, AMCOM decided to invest $500,000 to $1 million in additional network security measures. AMCOM selected Intergraph to help establish a structured IA program to support its 16,000 network users. To augment the program, the AMCOM Intelligence and Security Directorate established a Local Computer Incident Response Team (LCIRT), which provides automated information system support and resources for AMCOM sites in Pennsylvania, Texas, and Illinois. Intergraph supports the LCIRT on-site through technical guidance and advice to AMCOM customers on automated information system matters related to all research, development, and acquisition mission programs.

Rather than viewing IA as a series of isolated steps taken on demand to counter known threats, AMCOM and Intergraph are approaching security as a continuous life cycle of process improvements. The LCIRT and Intergraph worked together to build an integrated, continuous process of risk reviews, policy development and application, technology and process implementation, training, incident response, and accreditation to support various areas of AMCOM's network.

Services Provided:

- Information security assessment
- Process development for information security life cycle
- On-site technical guidance and support to Army Local Computer Incident Response Team (LCIRT)
- System consulting and monitoring

Key Benefits:

- Prevention of successful hacking attempts
- Increased information security
- Decreased security breaches

Profile:

Name – U.S. Army Aviation and Missile Command (AMCOM)

Web site – www.redstone.army.mil/new/AMCOM.htm

The U.S. Army Aviation and Missile Command (AMCOM) is a major subordinate command of the U.S. Army Materiel Command. In partnership with supported Program Executive Offices and program managers, AMCOM develops, acquires, and fields Army aviation and missile systems to ensure the Army's readiness and technological superiority in any future conflict.

Size – AMCOM is headquartered at Redstone Arsenal, a 38,000-acre installation located adjacent to Huntsville, Alabama.

Security, Government & Infrastructure

"It is essential to protect our information throughout the acquisition process to provide dominant weapons systems for soldiers on future battlefields," said Col. Douglas Brouillette, AMCOM's director of intelligence and security. "With the addition of Intergraph's support team, we have made rapid and significant advances in our ability to detect, follow-up, and prevent any loss of technology."

After evaluating AMCOM's network security for risks and liabilities, Intergraph and the LCIRT put in place a series of processes and measures to deal proactively with security issues. The LCIRT works closely with the Directorate of Information Management and the Corporate Information Center to identify, report, and respond to security incidents, and helps evaluate computer practices/ procedures, aid network support personnel, conduct security training, and administer security measures. The LCIRT works with organizations to develop and correctly apply policies, SOPs, security advisories, and military regulations in the network.

Intergraph also provides technical expertise in helping the LCIRT select, develop, and install software and hardware security solutions. These solutions include a diverse set of multiplatform hardware, operating systems, application software, network systems, and management tools. The LCIRT was involved in implementing a variety of systems and tools to support trouble reporting, change management, computer operations, config-uration management, data storage, administration, security, performance tuning, capacity monitoring, network mapping, and backdoor identification (modems, point-to-point connections, etc.).

The LCIRT currently monitors the content of more than 87 public Web sites at Redstone to ensure that information does not fall into DOD-restricted categories. The team actively monitors intrusion detection systems and Internet scanners and performs correlation analysis on the resulting log files. If there is an incident, the LCIRT determines intruder and target location, reports the information to the team leader for verification, and prepares an incident report. The intrusion detection engines are configured with various filters and are used to conduct the primary analysis of the data to determine events or incidents. Data and reports may also be prepared and sent to the Army for secondary analysis as necessary.

A More Secure and Accessible Network System

Since monitoring began, there have been seven or eight serious hacking attempts among the thousands of nonroutine connections detected, and none have breached classified information. While the number of attempted Internet intrusions continues to increase, the LCIRT has minimized serious security breaches through increased security education, monitoring, intrusion detection, and cutting-edge network security measures. The team has gained the respect of the user community by securing online data and providing technical guidance to organizations and partners with a "need to know." While the LCIRT has avoided potentially embarrassing, damaging, and unauthorized access of government network system assets, continued vigilance is necessary to offset the increasingly sophisticated intrusion attempts. Risk reviews, policy development, refinement, training, monitoring, and accreditation are part of a continuous, on-going process.

The Army Aviation and Missile Command (AMCOM)

AMCOM, a life cycle management command headquartered at Redstone Arsenal, Alabama, is a major subordinate command of the Army Materiel Command. AMCOM serves as the "Army's sustainment manager," keeping supported systems ready to fight.

Intergraph Security, Government & Infrastructure

Intergraph Security, Government & Infrastructure (SG&I), headquartered in Huntsville, Alabama, serves a broad range of clients, including local, regional, and national governments; businesses, both public and private; and security and public safety organizations. Intergraph SG&I focuses on providing software and services to enable our clients to make the right decisions at the right time using the right information.

For more information, visit our Web site at www.intergraph.com/sgi.

Images courtesy of AMCOM and the U.S. Army

FS087A0