

CASE STUDY:

E-COMMERCE NETWORK SECURITY ASSESSMENT AND DETECTION SERVICES

CLIENT DESCRIPTION:

Our client has management responsibility for running one the government's largest e-commerce systems, *GSA Advantage*.

CTA PROJECT DESCRIPTION:

Develop and implement a complete information security program for the agency, including policy, training and awareness, a Risk Management program, and a program to certify and accredit the client's automated processing systems general support systems and major applications. Further we have been tasked to implement an ongoing vulnerability assessment program and an intrusion detection capability within the organization.

PROJECT REQUIREMENTS:

The focus of the program is to provide protection, to ensure the availability, integrity, and confidentiality of mission-essential information and automated information system (AIS) resources. The CTA developed security program provides controls to prevent, delay, detect, identify, assess, contain, recover from, correct, and measure the loss of availability, integrity, and confidentiality of AIS assets due to attacks, malfunctions, and unauthorized activity.

SYSTEM ARCHITECTURE:

The *Advantage* system architecture is a large, complex, heterogeneous network consisting of thousands of workstations and hundreds of midrange servers and mainframe systems. Sun Solaris, Novell, Windows NT, and Unix operating systems make up the majority of the platforms used. Enterprise-wide networks and local area networks, with selective connectivity to the Internet, provide services to FSS internal and external customers.

WORK ACCOMPLISHED:

CTA performed technical work in a number of areas as discussed below:

Security Policy Generation

CTA revised and maintained top-level security regulations and policy directives. CTA supported this program objective by attending internal and external meetings, briefings, and information exchanges as directed by the government. CTA then developed an overall plan for implementing the Information Security Program, and coordinated it with appropriate client organizations. Specifically, CTA assisted in development of the overall client's Security Policy and Procedures. CTA then prepared specific security policy guideline documents for UNIX, Sun Solaris and NT platforms.

Intrusion Detection and Vulnerability Assessment

CTA has installed an intrusion detection capability utilizing the RealSecure IDS technology. Based on a pilot project, CTA assisted in the roll out of this capability to specified regions. Sensors have been installed at Ft.Worth, Burlington, Eagan, Roseville, CM4 and Chicago. CTA has installed and is using SNORT to supplement client-wide AIS Vulnerability Assessment Program. Continuous vulnerability scans utilizing a variety of tool sets are used weekly.

Network Security Policy

CTA is identifying and documenting security requirements applicable to network connection and use and developed a network policy. After the network policy was approved and published, CTA worked with organizational elements to develop specific procedures to implement the network policy within those organizations. CTA specifically, developed security configuration guides for UNIX, NT and Sun Solaris platforms.

Security Training and Awareness Program

CTA developed a security training program plan. CTA developed an initial security awareness course, a malicious logic course and a refresher training course.

Risk Management Process Definition

OMB A-130 mandated a risk management program be in place for each AIS to determine how much protection is required, how much exists, and the most economical way of providing the needed protection. Risk management is the process of establishing and maintaining information technology security within an organization. Risk management encompasses the entire system life cycle. CTA developed a standard risk management process for FSS that was based on a proven methodology and compliant with the GSA IL dealing with IT Security Policy.

Certification and Accreditation (C&A) Process Development

Certification is a comprehensive analysis of the technical and non-technical security features and other safeguards of a system to establish the extent to which a particular system meets a specific set of security requirements. Certification is done in support of the accreditation process and targets a specific environment. It includes risk analysis, security testing and evaluations and other activities as needed. Risk analysis is a part of C&A and provides a means of identifying and assessing system risks to justify safeguards. The objective of risk analysis is to ensure the security of computer systems is cost effective, up to data and responsive to threats. Accreditation is the formal declaration by a responsible organization that an AIS is approved to operate using a prescribed set of safeguards.

CTA produced a policy that defined a standard methodology for planning, performing, and maintaining C&A for a wide range of the client's systems. The policy provided an overview of C&A, identified the C&A approach, and provided instructions on how to conduct C&A. CTA has used the methodology to certify and accredit GSA Advantage, CM4 Lan, FSS-19, Customer Supply Center (CSC) and the Fleet Management System (FMS). CTA is currently in the process of certifying and accrediting other applications under our client's management.

BENEFITS TO CLIENT:

The benefits to the customer are numerous. First, having a solid policy upon which to guide their security program provided a basis for all program decisions, and increased the cost effectiveness of their security program. Second, having a well-defined structure for implementing the security program, and trained personnel who know where to go for what types of information and decisions, did much to focus and increase the overall security posture of the organization.