GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Bernard Jones
GIAC GSEC
Practical 1.4c
4 January 2005

Overview of DoD Defense in Depth Strategy

Abstract

The purpose of the paper is to introduce the of Department of Defense's perspective of defense in depth strategy and give an overview of how it is implemented through policy. Information assurance achieved through defense in depth in as policy established by the DoD Directive 8500.1.[1, 2] The mission is to assure the Department's information, information systems and information infrastructure and to support the Department's transformation to network and data-centric operations and warfare through the Global Information Grid (GIG) that allow information to originate from anywhere to be available on the network when required. The defense in depth strategy requires new and enterprise technologies that will interact on various level.

The Department of Defense (DoD) over the past decade, has become increasingly dependent on its computer networks. And thus, attacks on DoD systems has also increased.[3] At first, each individual agency developed its own solutions for protecting its systems. Now, Agencies such as Defense Information Systems Agency (DISA) and National Security Agency (NSA) worked together to provide security measures against this ever increasing threat.[4] In response, a defense in depth strategy was employed to protect its networks and information systems. The defense in depth strategy is a layered approach that uses people, technology and procedures to protect its network system.

Defenses in Depth Strategy

Defense in depth is an age-old military strategy. The most thought of visualization is a castle during the middle ages. The castle did not necessarily depend it wall to protect itself. It was surrounded by a moat, guard tower and bridge with a control access to the castle amongst other things.[4] If an enemy would want to defeat this, it would have to take in to account all these defensive measures put into place. Thus, DoD uses this strategy to defends its information networks.

Network Operations (NETOPS) provides the framework and procedure to manage the Global Information Grid (GIG). By integrating information assurance through a defense in depth concept with a network management and information dissemination management system, NETOPS is a key enabler for the Department in achieving information superiority and accomplishing its mission.

© SANS Institute 2005 Author retains full rights.

Today's technology trend plays a major role implementing defense in depth strategy. These technologies can be further divided into roles: networking and security. Networking technologies provide the infrastructure or backbone to move information from one system to another. These technologies include asynchronous transfer mode (ATM), ethernet, gigabit ethernet, wireless 802.11x standards, DNS security, Internet Protocol Version 6 (IPv6), and Internet Protocol Security (IPSec). Security technologies protect the information while it resides on a host or is transported throughout the network. These technologies include FORTEZZA based Public Key Infrastructure (PKI), virtual private networks (VPN), firewalls that enforce access control policies between networks, intrusion detection and prevention systems, virus scanners and secure applications such as secure socket layer (SSL), secure shell (SSH) and email encryptors.

DoD concentrated on three important principles to this strategy: people, technology and procedures. Analogous to the castle, technology represents the walls, moats, cannons and other weapons used during that age. The people maintaining the network must be properly trained and prepared to handle crisis as they arrive. The procedure and methods on how we defend on network must be well thought and planned prior to executing them.

From each of these three principles are used to defend the four key technical areas of the DoD security network: 1) network infrastructure 2) enclave boundary 3) computing environment and 4) supporting infrastructure.[1] Defending the network infrastructure relates to the roads that connect the castle and supports its outlying community (Everybody can't live in the castle). Defending the enclave boundary call for DoD the build walls and moats to protect its most important information and systems (i.e. King, Queen, etc.). Defending the computing environment focuses on protecting the chambers in the castle – the individual host used to by personnel in the DoD. Supporting the infrastructure is required the day to day operation to run the castle. Without food, water and supplies, the personnel who fight for us will eventually turn on us or leave their post.

The purpose of the defense in depth strategy is to protect the network and to ensure its availability when called upon to be utilized. The objective is to accomplish this in a layered approach. Each layer increases the defense posture around its critical assets and by multiple layers using varying security mechanisms. One layer is not solely depended upon to provide the defense but is taken into account when thought of in its entirety. Each layer is thought of from the perspective as information assurance pillars through people, technology and procedure.

Information Assurance Elements

People are the most essential part of the process. The best technology in the world is useless without personnel that administer them and the user that

© SANS Institute 2005 Author retains full rights.

need the access. People using technologies to conduct its operations are the strategy's central theme. People design, build, install, operate, authorize, assess, evaluate and maintain various security mechanisms. To gain and maintain the knowledge and expertise needed to perform these important tasks, comprehensive plan of education, training, practical experience and awareness training is required. The following are key components to this area in when discussing defense in depth

- Training
- Certification
- Awareness
- System Security Administration
- Physical Security
- Personal Security

Training enables DoD personnel to be adequately trained in the proper use and defense of its network. By creating an IA empowered workforce, the Department can meet and support demands of a changing enterprise. Certification documents that all personnel are proficient while use and defending DoD network systems. Awareness allows personnel to understand what technology can do for them and who authorized access to particular systems is. System security administration are those select individual trained in the operation and maintenance of security product used to defend the network in their respective enclave. Physical security restricts access to network devices which can compromise system integrity. Personnel security takes a look at users to defend against insider threats.

Perfect security can never be achieved especially with a single piece of technology. **Technology** component is more than just installing the latest and greatest security products. This involves full life cycle and support and development of these systems. It requires the evaluation and foresight to appropriately place these products in the defense in depth strategy. The key focuses in this area are

- Defense in Depth Strategy Layers
- Security Criteria
- Acquisition
- Risk Assessments
- Certification and Accreditation (C&A)

The defense in depth layer will be discussed in a later section of this paper. Each layer has an associated security mechanism that will be discussed in detail. The security criteria state whether or not a product performs at its expected level of performance. An example would be evaluating network and host based intrusion detection systems for a network or determine the best use of a virus scanner. This information is then passing on to the appropriate

© SANS Institute 2005 Author retains full rights.

acquisition professionals to procure the products that meet those requirements and specification. Crucial component is the risk assessment. Identifying threats and vulnerabilities and reviewing security polices give decision makers critical information in determining the right solutions and accepting appropriate level of risk when fielding security systems. DoD circular 5200.40 mandated the use of the DoD Information System Certification and Accreditation Process (DITSCAP) to certify and accredit all DoD systems.[5] The certification and accreditation (C&A) process validates that system perform in accordance with supporting documentation. This verifies that the system meets operational and security requirement put forth by the decision makers.

The **operation** component deal with implementation of security measures within an enclave. . These elements are

- Assessments
- Monitoring and Analysis
- Warning
- Response
- Reconstitution

Assessments continually conduct throughout the organization guarantee relevancy and that security mechanism in place satisfies new and existing requirements. Likewise, any change or addition requires reexamination in the C&A process. Intrusion detection systems and similar products allow us to monitor the systems, detect and analyze attacks and warn system administrators. When such an event has been determined to be an attack, administrators need to know how to respond appropriately. Responses need to be calculated to a predetermined best course of action to reduce damage and compromise of critical services. Reconstitution and restoral of services need to be planned in advance and conducted efficiently to ease delay when bringing systems back online.

IA Operations involves policy, procedures and execution. The policy drives operation by setting goals, courses of action and standards. It formally states the security requirements for the information systems, what must be protected, how resources are used and what must be done. Policy establishes standards that define uniform and common features and capabilities of security mechanisms, the rule by which to measure various dimensions of information assurance and the desired level of achievement. Standard operating procedures are then needed to ensure adequate implementation of the set policies. The procedures should define system configuration, deployment, routine operations and incident response and reporting. These defined procedures for addressing incidents are particularly crucial. After an intrusion is detected, incident information must be reported through established channels to appropriate authorities and specialized analysis and response centers. Incident response should begin at the local emergency response centers. Their actions should be

© SANS Institute 2005 Author retains full rights.

stated in detail the procedures and put in place immediately. Service wide center should be instituted where experts need to become involved when more sophisticated attacks are employed. Careful and timely decisions must be made concerning additional response such as: declaring higher level of information operations condition, isolate critical systems or appropriate response action. Operations also include improving situational awareness, conducting exercises and performing vulnerability assessment to improve the security posture.

Defense in Depth Strategy Layers

The basic idea of defense in depth strategy is applying multiple layers of defense to assure higher degree of reliance on critical information systems. At each layer, an appropriate security device is positioned to protect that layer. This strategy provides a level of resistance though might not be increasing as an attacker proceeds through an enclave. Defense in depth strategy categorize its four layers that must be defended

- Network and Infrastructure
- Enclave Boundary
- Computing Environment
- Supporting Infrastructure

The primary focus point of this goal is called Computer Network Defense (CND). . Using technology to defend the networks requires redundant and multiple paths more than one available transport medium. This allows continuous transmission coverage when interconnecting network components are down. Enclaves should be able to disconnect from external sources, filter certain segment traffic and control bandwidth. Automated tools for system management and monitoring should be used to analyze and collect data to observe for unusual occurrence and provide system status. Adaptive configuration management is a key component that entails active and passive defenses to correctly respond to real but changing demands while defending against threats.

The **network** and **infrastructure** layer includes the wide area network (WAN) within the Defense Information System Network and base or metropolitan area networks. The networks include technologies and devices such as asynchronous transfer mode (ATM), satellite system, Ethernet and wireless components. They carry voice, data and video information multiplexed over the circuit in a wide array of protocols and format. Complexity and speed is increased as innovative technology is fielded in various stages. The primary objective is to ensure the availability of the network to support DoD missions. Applying availability means controlling access the network devices, protecting network data management center from attacks and controlling the flow of information through out the network. To achieve this, there are multiple and redundant data paths. The network management system must be protected and

© SANS Institute 2005 Author retains full rights.

securely monitored. Each service and agency within the DoD must be certified and monitored to ensure the smooth connectivity through out the network. A connection approval system is in place ensures the every network connected adhere to the common security architecture and no conflict arises with other networks.

These strategic goals include:

- establishing GIG network defense architecture and baseline roadmap to respond to known and zero day threats
- developing and enforcing network defense policies across the enterprise to achieve the best readiness posture against outsider as well as insider threats
- evaluating and deploying network defense tools and capabilities in a coordinated manner to achieve a required operational capability
- establishing mechanisms and procedures within the network defense response action guidelines that effectively use tool to react and respond to anomalies and incidents.
- Mitigating the insider threat across the enterprise through implementation of processes, tool and operational capabilities (such principle of least privilege)

For classified network such SIPRNET (Secret Internet Protocol Network), this is a second objective. This layer must maintain its confidentiality of its data as it transverse the network. This means that the network must protect against interception of classified data. Inline and network encryption device provide this service. NSA is the agency that sponsors the development of these devices. [4]

The DoD network is layered in three hierarchies. Nonclassified Internet Protocol Network (NIPRNET) handles unclassified media traffic. It is often times confused as being the Web when it is just merely connected to it. SIPRNET handles data secret and below and Joint Worldwide Intelligence Communications Systems (JWICS) handles top secret information. Connections between the networks are closely watched through high assurance guards to protect from spillage of a higher classification system to a lower one. Special accreditation is conducted on these systems prior to being installed. Typically connections are encrypted to protect during transmission. [9]

Enclave boundary represents the local environment where the user works. Typically this is the base or unit structure where hosts and devices such as workstations, printer, and server reside. A wide range of services and protocols are at the user disposal but most commonly used ones are e-mail, web and telephone services. Defense of the enclave boundary is focused towards ensuring all systems outside that request access inside meet those security requirements. The boundary defense protect inside data from the dangers and hazards from the outside. They also protect systems that do not have their own

© SANS Institute 2005 Author retains full rights.

self defense capabilities. The enclave boundary usually has one or few connection to the network that is monitored and protected against attacks. Typical forms of attacked are e-mail embedded viruses and unauthorized login attempts via telnet. Security mechanism such as firewalls and guards protects against these intrusion. The unauthorized disclosure of information is also protected against in this layer. Information is monitored to ensure only authorized user have access at the appropriate level.

The local **computing environment** is the last line of defense in the strategy. The computer is the central focal point of operation and must be prepared to defend against a wide range of attacks. Operating system and application security has vastly improved over the last few years. A number of vendors now have met the common criteria standards for security evaluation that was only present in few DoD products. The local computer can have host-based intrusion detection system and anti-virus scanners to check the workstation and files against malicious activities. Operating systems such as Windows XP now comes with security features installed or can be easily added on.[8] Smart cards support authentication to verify that the user is allowed access to the system. Access control mechanisms are used to limit an authorized users' access to a workstations' files.[11] When properly implemented, these devices can provide a secure operating environment. Regardless of the number of security device are in place, user are educated to good security practices. Likewise, the proactive administrator must regularly audit logs and password and keep their systems updated with latest patches and virus signatures. [12]

The **supporting** or administrative infrastructure layer has two components, cryptographic infrastructure and intrusion infrastructure. The cryptographic infrastructure supports all key and certificate management commonly known as Public Key Infrastructure (PKI) [3,6] It is responsible for providing certificates used by applications to encrypt data. It also supports data protection and authentication algorithms. The Department has invested heavily in PKI, biometrics and Common Access Cards (CAC). Certificates are securely distributed and stored on directory servers and physical tokens such as smart cards allow users to access their respective enclave. An IA architecture will rely on a plug and play protection to enable devices to be reconfigured for security purposes and have strong authentication and authorization built in to make use of a Security Management Infrastructure (SMI). DoD has installed dedicated intrusion infrastructure to detection, reporting and response to instructions on DoD network systems. This infrastructure allows for the quick detection and reaction to intrusions. Host and network based intrusion detection systems correlate data to provide network management centers operational situation awareness. This infrastructure also include computer emergency response teams (CERTS) and their knowledge of attacks to network intrusion. [10]

© SANS Institute 2005 Author retains full rights.

Conclusion

An overview of how the defense in depth strategy is employed by the Department of Defense through information assurance measures was presented. The three measures that information assurance is implemented are through personnel, technology and its operation. The defense in depth strategy is applied in layers which focus on the following technical areas: network & infrastructure, enclave boundary, computing environment and supporting infrastructure. These measures are implemented through various security and network technologies that are in use and widely available

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Reference

[1] Ashley, Bradley K. and Jackson, Gary. “Information Assurance through Defense in Depth” URL: http://www.iwar.org.uk/infocon/dtic-ia/Vol3_No2.pdf , Fall 1999.

[2] United States. Department of Defense. Information Assurance. August 2002. URL: http://www.dtic.mil/whs/directives/corres/html2/d85001x.htm

[3] Galik, Dan. “Defense in Depth: Security for Network-Centric Warfare” April 1998, URL: http://www.chips.navy.mil/archives/98_apr/Galik.htm

[4] Onley, Dawn “NSA to take lead on Defense info assurance” Government Computer News. December 2004. URL: http://www.gcn.com/vol1_no1/daily-updates/31383-1.html

[5] United States. Department of Defense. DoD Information Security Certification and Accreditation Process (DITSCAP), December 1997 URL:http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf

[6] Hazelwood, Victor “Defense-in-Depth: Information Assurance for 2003” August 2003, URL: www.sdsc.edu/~victor/**Defense**In**Depth**WhitePaper.pdf

[7] Brooke, Paul. "Building an In-Depth Defense." Network Computing. July 2001. URL:http://www.networkcomputing.com/1214/1214ws1.html

[8] Strauber, Randy “ Defense in Depth” May 2004 URL: http://www.ebcvg.com/articles.php?id=219

[9] United States. Department of Defense. Information Assurance Strategic Plan V1.1 January 2004, URL:http://www.defenselink.mil/nii/org/sio/ia/diap/documents/DoDIAStrategicPlanJan04.pdf

[10] United States. Chairman of the Joint Chiefs of Staff Manual. Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND), August 2004, URL: http://www.tricare.osd.mil/tmis_new/ia/m651001.pdf

[11] Schweitzer, Douglas “The defense-in-depth approach to malware” May 2004, URL:http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C93274%2C00.html?f=x73

[12] Snyder, Joel “Turning the Network Inside Out” Information Security. June 2003 URL: http://infosecuritymag.techtarget.com/2003/jun/cover.shtml

© SANS Institute 2005 Author retains full rights.