Global Information Assurance Certification Paper

Defense in Depth – A Critical Case Study of a Large Enterprise
William A. McIntyre
May 2001

Introduction

Defense in Depth (DiD) is a layered approach to protecting computing assets which combines the capabilities of people, operations and security technologies to establish multiple layers of protection. DiD can also be considering a security strategy identifies and manages the risk of expected threats through use of multiple layers of protection. This paper is a case study of the Defense in Depth as implemented by our security organization, tools and technology. A comparison with business best practices is included at the end of this document.

Current Approach

Our organization has a central corporate infrastructure security group with three main subgroups. One group is responsible for overall program management, security education/training and executive security awareness. While security needs to be a corporate wide mindset, the current focus of our security awareness strategy is to target our executive management team. The second major security group in our organization is responsible for overall policy and procedures. Corporate risk assessments and business impact analysis are also part of the policy groups responsibilities. The third security group is the operations group. Our security operations group is responsible of the implementation and monitoring of our infrastructure security. While all three groups described above are essential to an affective enterprise security program, the remainder of this paper will focus on the efforts of security operations group and how they are implementing a DiD security architecture.

In order to properly support the security operations of our large enterprise, we have divided our central security operations organization into four teams. The first team is responsible for the Computer Incident Response Team (CIRT) and for developing and deploying security operations centers. This group also is tasked with recommending and implementing the underlying tools necessary to effectively support our security operations centers. Our CIRT team not only responds to incidents for risk mitigation but also provides vulnerabilities research and assessment. This analysis is shared amongst the other teams within our security group and enterprise. One of the analytical tasks our CIRT performs is to follow-up on any virus detected coming from internal sources. The CIRT team is also responsible to ensure that all firewall logs, server logs, DHCP logs and router logs are reviewed for anomalies and security events.

Our next security operations team is our perimeter protection or internet access group. They support all firewall technologies, caching proxy servers and perimeter virus scanning tools. Our perimeter protection defenses include virus scanning of all email messages. This group is also responsible for our secure enclaves project and for

blocking external access to undesirable web sites. Our enterprise has been directed to use "due diligence" by blocking access to certain external web sites. Web site blocking also deters our employees from visiting sites that might infiltrate our network with malicious code. The support and monitoring of the intrusion detection sensors is also accomplished by this group.

The third major group within our infrastructure security organization supports all the various remote access capabilities we currently support including PPP, VPN and dedicated business partner connectivity through leased lines and dedicated firewalls. This group is studying other VPN implementation configurations for business-to-business application as well. All network connectivity requests are reviewed by a Network Connectivity Review Board (NRCB) which is directed by this groups manager. NRCB standards are specifically documented in policy which define what sort of connectivity is always allowed. All other requests go through a formal review process.

The fourth major group with security operations supports in-depth on site penetration testing, high risk remote vulnerability testing, host based intrusion detection and server hardening. Enforcing policy to minimize "backdoor" hazards from notebook computers, personal software, pocket PC's, PDA's, and other similar devices continue to be a challenging and increasing effort shared across our teams.

Layered Architecture

Our network security follows the industry best practice by implementing layers of security and detection. Firewalls are an important layer to our DiD strategy but are not be relied upon as a single defensive solution. Our internet boundary is composed of a series of firewall technologies subnets and transfer networks. Our DMZ was originally setup to avoid relying only on one type of firewall technology, to distribute traffic for performance and to avoid unnecessary traffic flow. This approach to perimeter protection includes a firewall complex composed of redundant border routers utilizing tight access control lists, packet filtering firewalls and application layer proxy firewalls. None of the firewalls or infrastructure component management ports are accessible from the internet. Only encrypted sessions from an explicit internal security administration subnet are allowed to access any of the infrastructure devices including firewalls, transfer network switches and routers. The number of externally advertised IP addresses is kept to a minimum by using a series of non-routable internal DMZ transfer networks. Separate subnets are used for externally facing production servers, test servers and applications. The external domain naming server denies zone transfer requests to make network reconnaissance work more difficult. Firewall rule management is critical and all firewall administration is centrally controlled from one corporate group. Firewall rules are close by default and then selectively opened as required. Our centrally managed perimeter group uses a change control mechanism and deployment scripts for firewall rule distribution. We scan for malicious code both inbound and outbound through our mail relays.

Secure Enclaves

One of the security layers that we have added internally in our enterprise is the defensive mechanism we call secure enclaves. While many organizations have either a false sense of security about their internal critical systems, we have taken a proactive stance to protect our critical systems. These islands of protection isolate our critical servers inside an area of our infrastructure protected with firewall technology, internal intrusion detection. Secure enclaves define an additional level of trust and another layer of protection in our DiD strategy. Secure enclaves are one implementation strategy to avoid the hard exterior and soft interior levels of security. We have found that discussing the need for secure enclaves itself has increased security awareness inside our organization.

A secure enclave is more that just implementing a firewall to separte a portion of our intranet. Our requirements for a secure enclave inlcude a firewall guardian device but also include an network intrusion sensors inside the enclave. All machines inside the enclave have to be hardened to agreed upon standards prior to inclusion inside the enclave. Each secure enclave is required to have all three key components. We currently are deploying secure enclaves around all mail servers and other critical national applications. Security management is another area where secure enclaves are planned.

Network Based Intrusion Detection

Network based intrusion detection sensors (IDS) add another layer of protection through needed visibility. We have deployed IDS both inside and outside of our perimeter DMZs, within all secure enclaves and at key locations where critical sites are directly connected to our network backbone. The external sensors give us visibility as to what attacks our coming against our enterprise. The internal sensors are used for forensics to study if intruders having breached our perimeter and also to determine if any unauthorized activity is occurring from inside our network against external targets. Also the performance and ruleset used in our firewall complex can be verified by comparing theses two sensors. IDS signature maintenance is necessary yet time consuming effort.

Vulnerability Assessment/Penetration Testing

Another key component to our multi-layer approach in our enterprise security strategy is the ongoing vulnerability assessment and penetration testing efforts. We are actively performing high risk, remote vulnerability scanning of all sites. In addition we also perform onsite in-depth vulnerability and penetration testing on a smaller number of representative field sites. We test for policy compliance, standard configuration and hardening adherence, physical equipment access control in addition to other known potential system vulnerabilities. All infrastructure devices are testing and monitored to

ensure that both policy and hardening standards are maintained. All sites within our enterprise are being scanned on a perpetual rotating basis. Local Information System Manager and system administrator's assist in closing vulnerabilities as discovered in addition to maintaining security standards compliance and working to improve security awareness.

Host Based Intrusion Detection

Detecting security events on the host is yet another layer of defense we are currently deploying. We are in the evaluation phase to determine the best approach and tools to accomplish this additional protection to our network. We expect to deploy some form of HBID capability one all critical server in our enterprise. We are also considering the cost and benefits for more wide spread deployment. Our host based intrusion detection efforts are closely coordinated with other of our Information Technology engineering groups.

Hardening Standards

Consistent, tested and proven hardening standards add another very important barrier to our defensive security strategy. Today ten different operating system and twenty-six types of application server hardening standards are being developed and deployed. Router and switch hardening standards are scheduled for review and updates. All of these standards also are managed using a change control mechanism to ensure quality. Servers are dedicated by function and allowed to only host one type of application. For example we do not allow a web server to also be a database server.

Security Configuration Repository

While our effort to develop and utilize a security configuration repository is not directly another layer of defense, we have found that by improving our security tool set we are improving our security and thus adding to our network protection. After studying our various security efforts, many interdependencies were identified along with a core set of data necessary to effectively perform our security tasks. The result of this analysis was the definition of our security configuration repository, which is becoming a key tool for sharing security information and the base for performing necessary analysis. The security configuration repository is a data warehouse interfacing with many such existing enterprise sources as asset management, network events and critical system databases. Additional information is being added to our repository by configuring the various security tool outputs and by automating our processes through scripts. This concept is still being developed but it is envisioned to include a knowledge base of related text based. We plan to leverage the information in our security repository to scan for policy and hardening standard compliance.

Best Business Practice Analysis

Recent research has afforded the opportunity to compare our organizations current approach to the industries best business practices. In making this comparison, I found that many of Defense-in-Depth security strategy best business practices that I reviewed have been incorporated into our infrastructure:

- A layered architecture
- using multiple firewall technologies
- firewall rules and the hardening approach with everything closed by default and then only opening needed services and ports according to standards and review.
- limiting unnecessary traffic flow
- no management ports accessible from public subnets
- no DNS zone transfers allowed
- externally advertised address kept to a minimum
- firewall rules centrally managed with change control
- scanning both inbound and out bound messages for malicious code
- secure enclaves with hardened servers being implemented as additional layers
- enterprise wide vulnerability testing underway
- internal and external IDS

My research and analysis has also pointed out that improvements are needed in the following areas:

- Host based intrusion detection tool deployment
- Security management tools which scale to the size of our organization particularly in log processing and collecting and maintaining configuration data
- Identifying and closing backdoors
- Deploying an out-of-bandwidth capability for security and network management traffic
- Scanning additional ports for malicious code
- Security awareness needs to be an integrated part of our organizational culture

These deficiencies are now being studied and plans are being developed to address these needs.

Conclusions

Managing the security program for a large enterprise is a huge and ongoing task. We feel a DiD or layered approach is critical to discouraging hackers from attacking our organizational assets. Any security strategy, including a defense in depth approach, needs to be well thought out and centrally controlled. A Defense in Depth security strategy also needs to be proactive in its protection strategies and efficient in its response procedures.

As with many large organizations, our network security implementation is an ongoing effort; a work in progress. Our goal is to make security a way of life, a corporate worldview, starting with our executives and flowing down to all our employees. Corporate security needs to be everyone's responsibility.

References:

Allen, Julia; Christie, Alan; McHugh, John*, Intrusion Detection: Implementation and Operational Issues*, Jan 2001;
URL http://www.stsc.hill.af.mil/crosstalk/2001/jan/mchugh.asp

Convery, Sean; Trudel, Bernie; Cisco – Safe: A security blueprint for Enterprise Networks, URL http://www.itworld.com/WhitePapers/Cisco_SAFE.htm

Hartman, Scot; *Securing E-Commerce: An Overview of Defense In-Depth*, Mar 26, 2001; URL http://www.sans.org/infosecFAQ/start/sec_ecom.htm

Ia-std-editor@llnl.gov; *Statement of Direction: IA0401:Unclassified Computer and Network Security*, Feb 2000;
URL http://www.llnl.gov/projects/ia/standards/ia0401/ia0401.html

Manderscheid, Scott; *An Intrusion Detection System Process: Defense in Depth*, Feb 9, 2001; URL http://www.sans.org/infosecFAQ/intrusion/process.htm

McGraw, Gary; Viega, John; *Software Security Principles: Part 2 – Defense in Depth and Secure Failure*, Nov 2000; URL http://www-106.ibm.com/developerworks/security/library/s-fail.html?dwzone=security

McKenney, Brian; *Defense in Depth*, Feb 2001
URL http://www.mitre.org/pubs/edge/february_01/mckenney.htm

Potter, Al; *Differences between a firewall and a perimeter router*, Feb 1, 2001
URL http://www.securityportal.com/list-archive/firewalls/2001/Feb/009.html

Riley, Steve; *Using IPSec to Lock Down A Serve*, May 14, 2001
URL http://www.microsoft.com/ISN/Columniss/using_ipsec.asp?A=0

Robinson, Brian*; Firewalls: The First Line of Defense,* Mar 29, 1999
URL http://208.201.97.5/ref/hottopics/security/firewalls.html

Robinson, Clarence; *Info Security 2000: defense in Depth*,
URL http://www.aviation100.com/web04/yic/info.html

Ross, Seth; *TIPS: Defense in Depth Against DDoS*, Feb 18, 2000

URL http://www.pcusers.org/guardian.html

Ruthberg, Zella G; Tipton, Harold; Handbook of Informantion Security Management, Boston 1993; Auerbach Publications

Seifried, Kurt; *Defense in Depth:Cron*, May14, 2001
URL http://www.securityportal.com/articles/cron20010514.html

Sharlun, Glenn*; Defense In Depth: The Lessons from Troy and the Maginot Line Applied*, Nov 27, 2000; URL http://www.sans.org/inforsecFAQ/start/lessons.htm

Warfield, Michael; Defense in Depth, July 1999
URL http://lw.itworld.com/linuxworld/lw-1999-07/lw-07-ramparts-10.html

Well II, Dr. Linton; *The Changing Nature of Information Security*, Feb 2000
URL http://www.cisp.org/imp/february_2000/02_00wells.htm

Wilson, Michael; *Defense in Depth*, 1997
URL http://www.7pillows.com/papers/didfinal.htm

Wilson, Tom; *Lessons Learned in Microsoft Break-In*, Dec 4, 2000
URL http://www.sans.org/infosecFAQ/malicious/lessons.htm

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor