Global Information Assurance Certification Paper

Defense-in-Depth: From Risk Assessment to Self Assessment
A Dynamic Process

Kerrie L. Harney
GSEC - Version 1.2f

It is a long-standing and well documented principle of security that security in layers is the best way to protect information. After all, we would never be able to accept increasing levels of risk if we rested the burden of protection in one proverbial basket. In today's networking environment, more and more system administrators are using some kind of defense in depth. This may range from using a personal firewall with virus scanning software to a large, well-instituted and supported program that utilize every aspect of defense from policy to intrusion detection. Defense-in-Depth is a tool of information assurance that gives networks a fighting chance against would-be hackers. Defense-in-Depth utilizes layers of security giving the network administrator, users, and security personnel time to detect and react to intrusion and attacks. This greatly reduces the likelihood of a complete breach of system defenses. Ideally, the defense-in-depth measures you implement should buy you time to detect and respond to a breach, reducing its impact (Brooke). It would seem that the more sophisticated the defenses, the less chance of compromise of information and greater amount of risk acceptance. However, information will never be protected by technical means alone no matter how many levels of security may be built into the system. Superior implementations of Defense-in-Depth strategy integrate the capabilities of people, operations, and technology to establish multi-layer, multi-dimensional protection (The Joint Staff, p.2). This may seem easier said than done, but we must realize that information assurance is a dynamic process that requires constant evaluation and assessment. Employing an in-depth defense starts with a commitment to this process and a realization that defenses are more than just firewalls and encryption. Defense-in-Depth is a logic-based process that starts with evaluation of assets, needs and risks which translates to implementation of technical and non-technical countermeasures, and continues with constant self assessment.

Understanding and Accepting Risk

Once upon a time information security was motivated by risk avoidance. This entailed implementing whatever security countermeasures were necessary to ensure that information would and could not be compromised. However, in the digital age of fast-paced information exchange and an increasingly computer savvy user population, security does not translate to the old philosophy of the biggest lock and the thickest walls yielding the best protection. Instead of trying to avoid risk by protecting against all threats to information, we have moved to a risk management environment. This entails first identifying the criticality of the assets being protected, examining viable threats against those assets to determine current vulnerabilities in existing systems, and then employing the necessary security countermeasures to protect the information. Without big locks and thick walls, we have mitigated risk while allowing business and communication to flourish.

This may seem easier said than done. After all, threats to systems are as dynamic as a hacker's imagination. However, you have the resources and the talent of your entire organization to use

in the risk management process. In this situation managing risk requires security polices that balance usability and business requirements against risks. To balance out these risks, a collaborative process should be undertaken, including everyone with an interest, such as the system users, technical staff, and the senior management of the organization (Gardner). All of these people will play an important role in the identification of assets, threats, and vulnerabilities which will in turn determine what security countermeasures will be instituted on a network. Thus, security is an outgrowth of the risk management process.

Risk management is not just an exercise in network security philosophy. It is actually a part of your Defense-in-Depth that will impact not only technical security but also operational security and personnel security. The risk management process should be formalized resulting in the publishing and promulgation of security policy that will be used to regulate everything from system access to intrusion detection. By formalizing the process, your organization officially accepts risk at the organizational level and eliminates acceptance of risk at the individual level. This will be an important foundation to an in-depth defense of your network systems.

Layering Technical Security

Conventional network security defense begins with technology that can combat intrusion and damage to the network and at the same time ensure continuity of operations. However, we should not simply use some random combination of security features thinking that simply because we are using a variety of technical defenses we are implementing Defense-in-Depth. Instead we must use what we have learned from our risk management process. We have already identified the risks and threats against our network. Now we must plan our defense. The first step is to understand exactly what we are defending by mapping out our network and establishing a baseline blueprint of our system configuration. We may be setting up hardware from the ground up or we may use network mapping tools to determine what is on an existing system. In each case we must ensure that we understand the configuration of our network. Network mapping software can be continually used to detect vulnerabilities on a system and uncover unauthorized changes to system configuration.

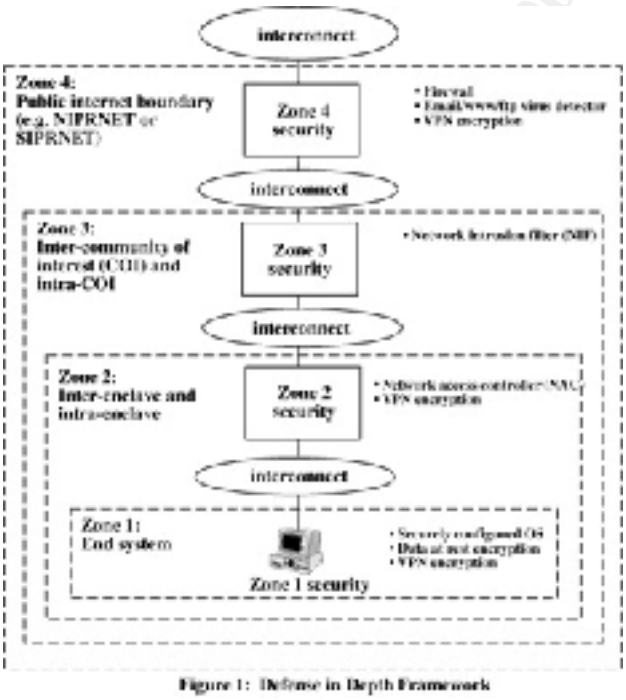

Figure 1: Defense in Depth Framework

The United States Department of Defense has long dealt with defending against intrusion of its networks. As a result, the strategy of Defense-in-Depth is now a widely used tool for information assurance. We will use the Defense Department's model of defense to understand the use of layered security features. Figure 1 (Galik) demonstrates how layers or "zones" of defense have been created to protect the "End System" and the communications between the zones. Protection extends from the most remote systems to the desktop. Like most

perimeter defenses, a firewall is used to establish a perimeter from the public internet. All traffic to the internet is routed through the NIPRNET (Unclassified but Sensitive Internet Protocol Router Network). In this outermost zone "defenses that are most appropriate here include firewalls, Virtual Private Network (VPN) encryption, content checking, and source authentication for routers and DNS" (Galik).

Additional internal firewalls have also been established to protect data and detect unauthorized access between user enclaves from inside the network. In other words, just because a hacker may have penetrated the outer perimeter, there are additional layers of security still intact.

In addition to the use of firewalls, intrusion detection and encryption are used in each zone to protect communication and detect unauthorized access. The Defense Department learned valuable lessons in the case that has come to be known as "Solar Sunrise." In this situation hackers were successful in exploiting a vulnerability in network domain servers running the Solaris operation systems. By exploiting one vulnerability the hackers were able to launch attacks against several key systems. As a result the Pentagon improved indication and warning systems specifically using technology that aided in characterization and attribution of attacks (Robinson, p.2).

At the desktop level we can use additional technical resources for protection. Most notably is the encryption of data stored on the desktop. Should an intruder penetrate through the firewalls and evade detection they would still find that data was being protected at the local level. In addition to host encryption, the use of virus detection software is a must. This will not only protect systems against malicious logic from outside the network, but it will protect against the introduction of malicious code from the inside. This is a very common scenario in which a system user introduces media onto a system without first running a virus scan. As a result, malicious code can spread quickly from inside the network. It is also important to update virus signature files on a regular basis.

Administrators should also consider methods of identification and authentication. Just as guards control access to buildings, an in-depth defense will implement means for authorized users to be identified and authenticated by the system. Administrators should have control over user accounts, and good password policy should be utilized. Most operating systems have built-in password strength requirements and will not allow duplication or reuse. One overlooked, but effective, countermeasure is to disable group or generic accounts built into the operating system. There may be generic accounts built into software that you are not even aware of, but I can assure you the savvy hacker is definitely aware. One good web resource for checking for the existence of group accounts is http://security.nerdnet.com/rawdump.php which lists the default passwords for operating systems.

There will always be a tendency to overcompensate with technical security. This can be the Achilles heal of your defense since the tighter the defense, the harder it will be to communicate and do business. This also leads to increased circumvention of security from the inside. All of this could lead to a fairly simple compromise in a system's defenses but if sound risk assessment has been accomplished, implementing the right technical security needed to protect information will allow business to flourish

.

Non-Technical Countermeasures

In a world of bits and bytes we may often forget the fact that we are not fighting against technology that has gone bad. We are fighting against people motivated by malicious intent who would use technology to hurt our business and steal our information. We must incorporate layers of security into our defenses that will combat these aspects of information warfare in addition to the technical threats. Unfortunately these are sometimes the easiest to identify but the hardest to control. We cannot always control the actions of people who have been given trusted access to systems and networks nor can we control the needs of business over the prudence of security. Even still, we can be as diligent as possible to include non-technical defense such as personnel and operations security into our Defense-in-Depth.

One of the most important aspects of Defense-in-Depth is the involvement of an organization's personnel in the security process. After all, these are the people who actually have access to the information and use the systems on a daily basis. Every system user needs to understand there is a responsibility to participate and encourage compliance with security policies and procedures. As employees, they are obligated to comply, but people are not often motivated by mandatory compliance requirements. Network defenses will truly be enhanced when employees are motivated (not scared) to adopt a commonsense approach to security and trained to recognize possible security problems. This can be accomplished through an awareness and education program. This training should not just teach information systems security as just another policy of the organization, but should highlight the consequences of poor security. This includes emphasizing that if proprietary information is lost, so are jobs. Each employee is not just protecting the company's assets but is protecting his/her own asset by ensuring a competitive stance in the business world. Planting seeds of awareness will lead to employees reporting everything from suspicious events to challenging access authorizations to systems.

In addition to user education, the system administrators must also set continuing education and awareness as a high priority. The threat environment will be constantly changing and the systems administrator will need to stay current on threats, vulnerabilities, and countermeasures. There are a great many web-based resources that can help the administrator maintain an edge against threats. These include incident monitoring sites like http://www.incidents.org, research and education sites like the National Institute of Standards and Technology - Computer Security Resource Center at http://csrc.nist.gov, and information sharing portals like http://www.inforwar.com.

One non-technical countermeasure often overlooked in Defense-in-Depth is operations security. This ranges from physically protecting the hardware of a system to the promulgation of security policy. Access to system hardware should be limited to necessary personnel and ideally protected in locked rooms.
Another operational defense is frequent auditing of the network. Although the word may strike fear in the hearts of administrators, it is probably the best way to maintain continual awareness of system configuration and detect indicators of suspicious activities. There are a great many software utilities that can be used to help administrator review what can be large amounts of

audit records. Title like Tripwire allow administrator to focus on certain audit items and provide a greater change of finding an anomaly or suspicious event.

Even though risk determinations have been made and technical and non-technical countermeasures have been put into place, the process of Defense-in-Depth is not over. Defense of the network will only be successful with continual self assessments and re-evaluation of policies and procedures. Through formal self assessments, administrators can determine what countermeasures are working well to protect information and even what countermeasures are inhibiting communication while providing minimal security. They can they react and fine tune defenses to meet the changed environment. In the example above we discussed the government's model for layered security as employed in the NIPRNET and SIPRNET. However, the Defense Department realized that a reliance on isolation of systems and heavy use of encryption was not an effective strategy for information assurance. What they did not count on was the high level of vulnerability from accidental or malicious threats from insiders (Slabodkin). As a result, greater emphasis was placed on access control, user education and awareness, and higher levels of internal auditing. In this situation, Defense-in-Depth was assessed, re-evaluated, and the necessary changes were made to strengthen defenses.

Conclusion

The only constant is the constant of change. Implementing Defense-in-Depth will require an organization to traversed an exhaustive and complex security process that will take the talents of a multitude of personnel and countless hours. Yet, we must be ready and willing to accept the fact that our threat environment will always be changing and evolving. Although Defense-in-Depth is a powerful and necessary strategy to help manage risk and protect assets, it is more than just a plan. Defense-in-Depth is a dynamic effort that involve a long term commitment to technical, personnel, and operations security. Still, it is a small price to pay for information assurance.

References:

Brooke, Paul. "Building an In-Depth Defense." Network Computing. July 9, 2001. URL: http://www.networkcomputing.com/1214/1214ws1.html (October 20, 2001).
.
Galik, Dan, Capt., USN. "Defense in Depth: Security for Network Centric Warfare." URL: http://www.norfork.navy.mil/chips/archives/98_apr/Galik.htm (October 20, 2001).

Gardner, Rick. "Computer Network Security Must be an Ongoing Process." Houston Business Journal. 16 March 2001. URL: http://houston.bcebtral.com/houston/stories/2001/03/19/focus2.html (October 29, 2001).

Robinson, Clarence A. "Info Security 2000: Defense in Depth." URL: http://www.aviation100.com/web04/yic/infor.html (October 29, 2001).

Slabodkin, Gregory. "NSA Officer: Defense systems are at risk from internal threat". Government Computing News. 8 February 1999. URL: http://www.gcn.com/archives/gcn/1999/February8/45.htm (October 29, 2001).

The Joint Staff. " Information Assurance Through Defense in Depth." February 2000.

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event