Global Information Assurance Certification Paper

Defense in Depth: A Primer

Security Essentials Practical
Charlene VanMeter
(410) 540-4801

Introduction

As we begin the 21st century, we have seen a growing trend to connect our networks. We connect our internal business LANS in order to share information across departments in our company. We connect those networks to the external world to communicate with other businesses and to access information on the Internet. As we have increased our network connectivity, protecting those networks becomes extremely important. The more connected we become, the more vulnerable we become to attack – both internal and external. Simple solutions to security are rarely sufficient, particularly since breaches in network security can result in real losses: system downtime, lost productivity, public exposure of sensitive information, and loss of proprietary information. Taking a Defense in Depth approach to network security means that you don't rely on a single technique or mechanism to protect your network, therefore lowering our susceptibility to attacks.

This paper briefly discusses the principle of Defense in Depth. The first section defines Defense in Depth. The second section explains the importance of knowing your security requirements (or goals) in order to determine the types of layered defense you may want to use to protect your network. The third section examines three aspects to a Defense in Depth approach to network security.

What is defense in depth?

Defense in Depth is a term used to describe a critical approach to information assurance in today's world of connectedness. Defense in Depth is "a term borrowed from the military used to describe defensive measures that reinforce each other, hiding the defenders activities from view and allowing the defender to respond to an attack quickly and effectively. In the network, defense in depth describes an approach to network security that uses several forms of defense against an intruder and that does not rely on one single defensive mechanism."[1]

The underlying principle to Defense in Depth is implementing layers of security to protect a network. No mechanism exists for completely securing a network, particularly if you are connected to the Internet. It is not possible to identify every single flaw in a network and to compensate for them, and there is no single mechanism that can adequately protect a network (unless security is not really an issue). However, it is possible to implement security and detection as a set of layers such that a hole or flaw in one layer will be covered by other layers. A potential attacker will be ignorant of the security mechanisms in place and will have to break through all layers of security without being detected. Consequently, Defense in Depth improves the network security.

[1] Dyson, Peter. "Dictionary of Networking". 13 Feb 2001.
URL: http://www.smart-media.net/connolly/netdictionary/Terms/2461HTML-725.html (16 Feb 2001)

Defense in Depth: A Primer

Understanding your Security Goals

To implement Defense in Depth, you first need to know your network security goals (or requirements). Armed with this information, you can identify what security products or techniques will best meet your needs. The degree of security needed depends on the business using the network. A Department of Defense network may have significantly greater security needs than a university network

The first step in securing your network is to generate a security policy. The security policy is a comprehensive document that defines what needs to be done and by whom. This document defines your security requirements (or goals). The detail in this document will help determine the level of security needed and drive the decisions about the products that you will buy or the techniques that you will employ to protect your network. This document also identifies key personnel involved in protecting your network security from management to the system administrator to the user.

The security policy will identify what you need to protect which includes the data, the equipment, and even the building. It also identifies who may do harm to your system. If you are connected to the Internet, a hacker from outside may do you harm. However, disgruntled employees inflict over half of the intentional harm to networks. And then, of course, there is unintentional harm that results from accidents or too little knowledge. The security policy also assesses the potential threats to the system and ranks these threats according to the potential damage they pose. And the security policy prioritizing everything you are protecting according to its relative importance. This step assures that you focus your efforts and budget on the most important issues. This is key when you have a limited budget.

Implementing Multiple Layers of Security

Once you have documented your requirements in a Security Policy, you are then ready to start implementing your security policy. And of course, your implementation builds successively stronger layers of security that work together to reduce the threats into "manageable pieces". The actions taken to layer network security can generally be classified into the falling views: personnel, technology and operational.

Personnel

When considering network security, we frequently think of technology: passwords, routers, firewalls, and intrusion detection. But personnel issues are a very important and often-overlooked aspect of network security. All personnel must be involved in security from the user to the security officers. The users are key to maintaining secure environments and must be indoctrinated in the company's security practices and procedures. This includes such things as not allowing unauthorized personnel to access their accounts, opening an insecure access, unauthorized network modifications, following password practices, not selecting easily guessed passwords, and not sharing

passwords. System administrators or network administrators usually have access to all systems. When the security needs are critical, it is typical and actually important to have a separate security administrator. Whenever an event occurs, such as slow performance of the network, the system administrator will focus immediately on trying to improve performance. A security administrator will focus on ensuring that the poor performance is not the result of a security breach. There can also be conflicts when a security mechanism dedgrades the network performance. In some organizations, may have an Information Systems Security Officer (ISSO) who is responsible for all network security infrastructure issues. Untrained administrators and ISSO's can wreak havoc on the functioning and the security of the network – unintentionally. If a system, or even worse, a security features is configured wrong, a security flaw can be unintentionally introduced into the network. Therefore, ensuring that our administrators receive adequate training is another significant element of security.

Technology

The technology aspect of security refers to all of the technical solutions that we use to implement security. Technology can be described by the following layers: defending the networks, defending the enclave boundary (if it applies), defending the computing environment, and the infrastructure required to support or implement these defenses.

Defending the network refers to the security measures required to defend your business's external network connection. Firewalls, Intrusion Detection Systems, auditing, virus scanning and encryption are several examples of ways that the network connection can be defended and added layers provides greater and greater security for your network connection. If your security policy limits traffic into and out of your network, you might install a firewall between your network and the Internet. If you are protecting critical data on your network, you may want to run an intrusion detection system as an additional layer to your firewall. The intrusion detection system can monitor the network connection for suspicious activity, particularly an intrusion into your network; and take pre-defined actions based on what if finds. Auditing (or creating logs) of activity. Firewalls and Intrusion Detection Systems maintain their own logs, but additional logs may be deemed necessary to monitor the security of the overall network. For example, an audit could detect the addition of unauthorized hardware or software to the network. . For an additional layer, encryption can be used to transform a data file into an unreadable mix of letters and characters. Encryption can be used between known users to ensure that their communications are private and to authenticate the identity of the sender to the recipient. For yet another layer of security, virus scanning can also be applied at the firewall level to block known viruses, after decrypting packages.

Defending the enclave refers to the security measures required to defend your business's internal networks. An enclave generally refers the internal network to include local area networks if they exist. Connections to the local area networks can be secured in the same manner as the connection to the external environment, using firewalls, intrusions detection systems, auditing and virus scanning. For a particular private enclave, encryption may be applied as well. Internal threats apply in this environment. This

includes the unintentional damage resulting from an insecure environment to intentional damage resulting from the actions of a disgruntled employee. The damage inflicted by a disgruntled employee can be contained by having enclaves for each department and using access privileges to limit access to critical or private data.

Defending the computing environment refers to protecting the application hosts and servers. Examples are the main server for a LAN, the e-mail server, and the web server. Intrusion detection systems, virus scanning and encryption can protect the computing environment. The hardware and software must be configured properly and security must be taken into account when installing hardware and software.

In fact at each layer, the configuration of the security mechanisms must be set up correctly to eliminate unintentional breaches. As stated earlier, if equipment, an operating system, or other software is configured incorrectly, a security flaw can be unintentionally introduced into the network. Which means that it is very important that our administrators receive adequate training. Again, it is important that the administrators are properly trained. Administrators also need to keep abreast of upgrades that patch known holes or bugs, and guarantee that these patches are applied.

The relationships between the security mechanisms must also be taken into account when protecting the entire network. Before security is implemented, consideration must be given to how these mechanisms work together to protect the network. For example, you need to ensure that when you are logging events that it is possible to trace the path or effect of an anomaly between layers.

The support infrastructure aspect refers to those mechanisms or procedures that must be implemented to support the other three layers (defending the network, defending the enclave, defending the computing environment). This layer includes Public Key Infrastructure, network and security management, and analysis of all audits. Public Key Infrastructure refers to the techniques and processes that are associated with implementing encryption. This includes the generation, distribution, control and accounting of the public key certificates that are required to encrypt files. Public Key Infrastructure provides the user with the ability to successfully apply encryption to his communications. In this context, networking and security management refers to managing the relationship between the two. As mentioned earlier, network management focuses on getting keeping the network up and running and on performance. Security management focuses on security. Sometimes a security mechanism degrades the network performance. So, it is crucial that these two areas work closely together. Analysis of the logs generated by the firewalls, the Intrusion Detection Systems and other audit logs is also provided by the infrastructure support. This analysis should be done on a regular basis to search for anomalies that weren't automatically rejected by these systems. Analysis of audits may uncover that the patches aren't being applied. Also firewalls and intrusion detection systems and whatever mechanisms you are employing must be routinely analyzed to ascertain that the rules are not in conflict. Over time, individual changes may conflict with each other and open an unintentional hole in the network protection.

Operations

The operational aspect of security refers to all of the day-to day activities that support the operation of performing network security. This layer encompasses the physical security and network security policies and procedures. Physical security governs access to the building itself as well as access to various departments or to rooms housing key equipment. As with the other elements of security, the level of physical security is driven by the size of the organization and sensitivity of the data. The network security policies and procedures encompass the network security policy as well as the associated practices and procedures that should have been recommended in the policy. The Network Security Policy was discussed at length under the section "Understanding Your Security Goals". The network security policy drives everything that your organization does to protect your network. It is the backbone of your network security activities. The security practices and procedures cover a wide gamut of activities. How often the Network Security Policy is reviewed and updates is one those procedures. How often for firewalls, intrusion detection systems and other mechanisms are reviewed and analyzed for proper configuration is another procedure that must be addressed. Establishing Configuration Control Boards to govern changes to the security and to the network design will help control what is added to network.

Conclusion

The most important aspect of securing your network is knowing what you need to protect and knowing the sensitivity to information residing on your networks; in other words, knowing your requirements. Once you understand the threats to your system and your weaknesses, a layered approach to implementing security is critical to protecting your network. This layering strategy recognizes that multiple vulnerabilities exist in your network, which cannot be protected by a single mechanism. In short, a Defense in Depth approach provides layers of barriers, when combined successfully reduces the vulnerability of your network by raising the probability that attackers will be caught as they break through successive layers.

Defense in Depth: A Primer

Sources

Alberts, David S. "Building Defense in Depth". Defensive Information Warfare. August 1996. URL: http://www.dodccrp.org/diwCH15.htm (12 February 2001)

Alberts, David S. "Building Defense in Depth". Defensive Information Warfare. August 1996. URL: http://www.dodccrp.org/diwCH8.htm (12 February 2001)

Blancharski, Dan. *Network Security in a Mixed Environment*. Foster City, CA:IDG Books Worldwide, Inc. 1998.

Dyson, Peter. "Dictionary of Networking". 13 Feb 2001. URL: http://www.smart-media.net/connolly/netdictionary/Terms/2461HTML-725.html (16 Feb 2001)

Green, Mike R. "Public Key Infrastructure" 27 March 2000. http://www.doim.army.mil/Conference/dc2000/Briefingsslides/PKIPanel/sld014.htm (16 February 2001)

Gerretson, Jim. "What Can Be Done". 5 June 2000. Briefing Slides. (20 Dec 2000)

"In-depth defense". 28 Feb 2000. URL: wysiwyg://fraTopic.144/http://www.windows.com/windows2000/en/server/help/sag_IPSECindepth.htm (16 Feb 2001)

Warfield, Michael W. 26 May 1999. "Securing Linux/Unix Systems". Internet Security Systems, Inc. URL: http://www.wittsend.com/mhw/1999/securing_linux/gfx029.html (12 Feb 2001)

Last Updated: July 26th, 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
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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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 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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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
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 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
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
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event