Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Information Security: Managing Risk with Defense in Depth

The expectation of always being connected via the internet, having instant information, and data sharing while remaining productive and efficient, comes with a substantial risk. As a result, we, as Information Security Professionals, are required to focus our attention on minimizing risk while maintaining the three bedrock principles of information security: Confidentiality, Integrity, and Availability. In order to accomplish this we are tasked with the design, implementation, and daily maintenance of a strategy know a...

Copyright SANS Institute
Author Retains Full Rights

AD

Information Security
Managing Risk with Defense in Depth

GSEC Practical Assignment
Version (1.4b)

Kenneth R. Straub
August 12, 2003

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Information Security - Managing Risk with **Defense in Depth**

Abstract

In the information age in which we live, we find more and more individuals, businesses, corporations, and countries becoming interconnected through the global network known as the internet. We have information on demand practically anytime, anywhere. The lifeblood of the global economy depends on the internet being available, and it's hard to imagine day to day life without email. The ideas of *always connected*, *instant information*, and *data sharing,* while remaining productive and efficient, come with a substantial risk. As a result of this, we, as Information Security Professionals, are required to focus our attention on minimizing risk while maintaining the three bedrock principles of information security: *Confidentiality, Integrity*, and *Availability*. In order to accomplish this we are tasked with the design, implementation, and daily maintenance of a strategy know as **Defense in Depth.**

The concept of **Defense in Depth** is to use multiple defense mechanisms in layers across your network infrastructure to protect your internal data, systems, networks, and users. We use multiple defenses so that if one defensive measure fails there are more behind it to continue to protect the assets. This paper will first give a detailed overview of risk/risk management & data classification and why we need the **Defense in Depth** strategy. Then it will layout the blueprint for **Defense in Depth**. Each layer will be identified and followed up with a description and/or best practice depending on the technology involved. There may be times throughout this paper when specific vendors and/or products are mentioned. This is not done as an endorsement of any kind. A conclusion section will bring the topic to a close, followed by a list of references, which were used to help support the document.

Defense in Depth

Information Security is about minimizing risk to an acceptable level while maintaining the Confidentiality, Integrity, and Availability of the systems and data. All systems have some level of risk. A completely secure, zero risk, system is one that has zero functionality. At a recent SANS Conference I attended it was simply put like this: *The only system that does not have an inherent risk is a system that is completely disconnected and powered off. Then the system is encased in cement and buried in your backyard*. Therefore, all systems have a level of risk associated with them. The security problems and pitfalls associated with systems fall under an extensive range of categories. A few of them are:

- Viruses
- Unpatched Systems
- Buffer Overflow Vulnerabilities
- Unnecessary services running
- Denial of service attacks
- Social engineering

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

It is in our best interest, and our employers' best interest, to implement a proactive **Defense in Depth** strategy instead of a reactive "put the fire out" strategy.

The SANS Security Essentials with CISSP CBK Volume 1 book states that:

"Risk = Threat X Vulnerability"
(Cole. Fossen. Northcutt. Palmeranz., P. 306)

High Risk	=	High Threat, High Vulnerability
Medium Risk	=	High Threat, Low Vulnerability
Medium Risk	=	Low Threat, High Vulnerability
Low Risk	=	Low Threat, Low Vulnerability

Threats can be thought of as anything that can negatively affect the Confidentiality, Integrity, or Availability of your systems and/or data. The two common threat types are physical threats (fire, terror attacks, floods, etc) and electronic threats (viruses, denial of service attacks, hackers, etc). There are two sources of threats, the external threat and the internal threat. A common misconception among many managers is that the internal threat is more a myth than a reality. To that I offer you the following quote from www.securityfocus.com, which summarizes a survey taken from the CPI/FBI:

> *"Although the vast majority of attention is given to protecting against external threats, insider attacks are a serious, and common, threat. According to a CPI/FBI survey, 59% of companies surveyed said they have had one or more attacks reported internally. Almost 8% of those companies reported 60 or more internal incidents."*
> (Einwetcher , http://www.securityfocus.com/infocus/1558)

Your particular situation may be unique, and therefore the threats to you might not necessarily be the same as to everyone else. Regardless of any uniqueness, it needs to be understood that threats exist for everyone.

Vulnerabilities are weaknesses in systems or devices that allow threats to compromise a system. These can be a result of services running, unpatched systems, poor configurations, etc. Just like threats, vulnerabilities exist in all systems. However, not all vulnerabilities are bad and have to be stopped. In fact some vulnerabilities are necessary to provide functionality and operations. It is when the vulnerability meets up with the threat that the Confidentiality, Integrity, and Availability of systems, and the data they hold, are in danger of compromise. Eric Cole stated at the SANS conference March 2003 in San Diego:

> *"If you reduce your vulnerabilities you reduce your level of risk."*
> (Cole, SANS conference March 2003 San Diego CA)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Vulnerabilities are really the only variable that we maintain some control over. Threats are always going to be there and, for the most part, will be out of our control. Therefore, a **Defense in Depth** strategy will take aim at the reduction, removal, and separation of vulnerabilities. The idea will be to reduce the risk to a low level by layering defense mechanisms. The primary objective is to remove the unnecessary vulnerabilities, and separate the business necessary vulnerabilities from the threats where applicable. In instances where this is not possible, or only partly possible, **Defense in Depth** will provide additional protective layers of defense as well as the all-important logging function. In the event of an incident response call, these logs will provide the necessary audit trail for forensic investigations.

Now that we've realized the risk we have by virtue of the threats and vulnerabilities that exist, we need to turn our attention to classifying our data. It is very important to classify your data in the design of your **Defense in Depth** strategy. Data classification, along with your Risk analysis, will determine where, and to what degree, your systems and data will be protected. Not all systems and data need the same degree of protection. Treating everything as top secret data will result in high implementation costs and could result in functionality that is too restrictive. Remember we are trying to minimize risk while maintaining Confidentiality, Integrity, and Availability. We need to provide this service within a reasonable cost and functionality. Submitting an information security project with a bloated cost analysis will be doomed from the start 99% of the time.

Data classification will vary from business to business. The U.S. Department of Defense uses a five-tiered classification set for all their data:

Top Secret
Secret
Confidential
Sensitive but unclassified
Unclassified

I would recommend the use of four levels of data classification. They could be Top Secret, Confidential, Sensitive but unclassified, and unclassified. Now that we've classified our data we can apply the risk model to it and come up with a reliable risk factor. Once done, we can prioritize the systems/data and start to line up our defenses.

Before we describe the different layers of defense, it's important to remember that when we design, deploy, and maintain a **Defense in Depth** strategy; our intent is to take a broad enough approach to cover all of the areas and requirements we identified. It should also provide the necessary redundancy to slow down an attacker so we can detect the attack and prevent it from doing any damage. The following defense layers will be presented in a list form, starting from a high level and working down to the data. There aren't any hard and fast rules to the order of the layers. For instance, it is a general practice to have a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

firewall as a perimeter defense, but that doesn't mean a firewall can't be used deep inside a network to protect a critical network or host. Each situation will yield its own requirements. Using some defense layers in multiple instances is not out of the ordinary.

Defense in Depth – Security Policies Layer

The policy layer is probably the most overlooked and misunderstood aspect of information security. Security policies should be the foundation of every **Defense in Depth** plan. One of the main purposes of security policies is to educate **all** users of **their** obligation to the protection of the technologies and business information. Security policies help protect both business information and employees in many ways:

1. They provide the guidance for what must be done to protect the business information stored on the corporate network.
2. They establish a set of rules of conduct for all users.
3. They provide authorization for the information security personnel to perform various duties such as monitoring, sniffing, probes, password cracking, etc.
4. They are the baseline for measuring compliance and enforcement.
5. They define the consequences of violations to the policies.
6. They act as a starting point to establish periodic review and updates for new threats and vulnerabilities, as well as improvements in meeting business needs and employee awareness.

When the security policy and its operational health are overlooked, information security is left to focus on the use of technology to prevent, and/or react to, security incidents. This is a backwards approach because poor policy decisions or operational practices can lead to circumvention of even the most robust technology put in place.

A Computer Weekly survey of 638 public and private sector respondents titled "Committing to security: A CompTIA Analysis of IT Security and the Workforce" states:

"In more than 63% of security breaches identified by respondents, human error was the major cause. Only 8% were purely technical failures."
(http://www.cw360.com)

These numbers reveal the fact that no matter how you look at it, the “human element” is always the weakest part of any security system. Because of this the process of designing policies should take into account, with more scrutiny, the human element. One must exercise caution though as this can be a double-edged sword. Security and policies are often viewed as obstacles to productivity, methods of controlling types of behavior, and big brother watching.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Other security policy pitfalls are: they're too restrictive, inconsistent, hard to understand, and unenforceable.

The SANS Security Essentials with CISSP CBK book, volume 1, states that:

"An effective and realistic Security Policy is the key to effective and achievable security."

(Cole. Fossen. Northcutt. Palmeranz., P. 339)

The policies themselves must be realistic and effective with achievable security goals. The more restrictive and complex a policy is the more likely it is to fail and lead to circumvention. Security policies must strike a balance between protection and productivity. Remember, the security policy is not the only means of defense. There are many others to put in place. Do not make the mistake of making your policies too restrictive, as if they are your only defense mechanism.

If you are new to information security and policies, there are numerous resources available on the internet for samples and guidance. The SANS website has a wealth of information pertaining to security policies. Keep in mind though that every situation is different, so all of these policies will need to be customized to fit your business needs. A dangerous practice would be to just copy, paste, and implement without fitting it to the business.

In general your security policies, once written, should have some, or all, of the following elements:

1. Should give a statement as to why the policy is needed.
2. Should give a scope of what, or who, it applies to.
3. Should clearly document the guidelines as to what is required.
4. Should identify any actions necessary, and when they are necessary.
4. Should reference supporting documents and policies.
5. Should list all responsible parties, and what they are responsible for.
6. Should document how violations will be handled.
7. Should give any miscellaneous information pertinent to any of the above items

Once policies are written they need to be fine tuned, so don't hurry to publish them. Fine tuning a policy can be one of the most important parts to policy development. Evaluate the policies with a checklist. The SANS Security Essentials with CISSP CBK book suggests that some of the fundamental things to check for are:

1. *Does it contain the expected elements listed above.*
2. *Is it clear.*
3. *Is it concise.*
4. *Is it realistic.*
5. *Is it consistent with other policies.*
6. *Is it in violation of local, state, or federal computer crime laws or regulations.*

(Cole. Fossen. Northcutt. Palmeranz.,)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Revise the document and evaluate again. The next step is to take the policy to a group of key users to read and provide feedback on their interpretation of it. Based on their feedback perform another revision and evaluation. This process will need to repeat as necessary until the checklist is satisfied and those key users understand the policy.

Once you have a final version of the policy it is time to get it signed and make it available to the user community. The common way of doing this is printing it and have people sign off that they received it. However, a more efficient way to push it to your users and keep track of who has read it is to use your intranet as the vehicle with a database to keep track of the users and the revisions.

Policies are living documents, always to be reviewed and revised. A policy program that does not review and revise its policies, on at least an annual basis, is setup for failure. Without a formal review you will have no way of knowing if the policy still meets business needs, if there is non-compliance, or if it is protecting against any new threats or vulnerabilities. A formal policy review will cause you to deliberately walk through the policy lifecycle of creation, implementation, enforcement, review & revise. Though this is a time consuming endeavor, it is one that will help ensure a healthy policy program for the future of your information security plan.

Defense in Depth – Strong Passwords Layer

Many companies rely only on passwords as their defense, and since the password is in essence the key by which authorized access exists, it warrants its own section as a defense layer. Strong Passwords will typically be specified and enforced with a Password security policy. Our goal is to make it difficult for an attacker to gain access, of any level, to a system with the use of an authorized username and password. Since usernames are typically easy to guess we will set out to make the password impossible to guess. The do(s) and don't(s) below, along with the guidelines that follow, will help accomplish this.

Strong Password DON'T list

- DON'T use any part of your username.
- DON'T use any dictionary words in any language.
- DON'T use any word associated with you or your interests.
- DON'T use a word with character substitution i.e. p@ssw0rd.
- DON'T write your password down on paper.
- DON'T store your password on any computer.
- DON'T use the 'remember my password' option.
- DON'T share your password with anybody.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Strong Password DO list

- Use a minimum of 8 characters
- Use at least three of the four classes listed below
  1. Upper case letters
  2. Lower case letters
  3. Numbers
  4. Special Characters (!@#$%^&*(){}<>,.;:"\+=-_)
- Change passwords every 60 days at a minimum

Guidelines

The easiest way to pick a strong password that is within the boundaries listed above, and easy to remember, is to use a pass phrase. A pass phrase is a phrase of words that you can easily remember. Then take the first letter of each word to create the password. Once you have it figured out, and at your discretion, use some form of character and/or number substitution. For example the pass phrase "I went to Florida 30 times before I saw Mickey Mouse" would yield a password of "IwtF30tbisMM" without the quotes. As you can see this is the beginning of a very strong password. It has 12 characters, it's not a dictionary word of any kind, it has no meaning to anyone and cannot have a meaning derived from it. We do not have to write it down to remember it because we know it by the pass phrase. Now in order to satisfy the DO boundary, we come up with a personal form of character substitution. For instance, every time the letter "t" is used substitute a "+". Since your first letter is I, and it is capital, make the other "i" capital for consistency and ease of remembering. Keep the proper nouns as capitals and you will have a strong password that looks like this:

Iw+F30+bIsMM

System Administrators should enforce strong passwords on all systems with the following criteria.

- Expire after 60 days minimum
- Lock out account after three failed attempts
- Log all success and failed login attempts
- Use password filters to ensure length and character inclusion
- None of users previous 6 passwords can be reused
- Passwords should have a minimum use of three days
- Enable strong encryption of all passwords (/etc/shadow; NTLMv2)

With the Strong Password created above and the enforcement on the server, it would be extremely difficult for an attacker to break in with a valid user name and password. If an attacker trying to crack passwords came up against our example the password would most likely expire before they could crack it and use it.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Defense in Depth – Perimeter Protection with Firewalls Layer

A critical and essential part of any Information Security plan is undoubtedly the firewall. Firewalls serve as the best protection control mechanism available in the information security arsenal. Commonly deployed at the perimeter gateway, the firewall stands as a traffic cop, allowing or denying access to and from different attached network segments based on the ruleset applied. While primarily used as gateway devices, it is not unusual to use firewalls internally to protect certain networks or individual hosts. Since firewalls play a major role in a **Defense in Depth** strategy, we will detail the three different types of firewalls.

Firewalls come in basically three types with various features. Depending on the type and feature set, they will provide some or all of these major elements of protection:

1. Reduce risk by protecting systems from attempts to exploit vulnerabilities.
2. Increase privacy by making it harder to gather information about the site.
3. Enforce an organizations security policy.
4. Log traffic for audit and forensic analysis.
5. Provide VPN/Encryption capabilities.
6. Perform Network Address Translation (NAT).
7. Provide Integration with content filtering systems.
8. Filter unwanted traffic

Firewall Type 1 – The packet filter

The packet filter firewall is a router (usually Cisco) using access control lists (ACL's). They are fast and generally low cost in comparison to the other types of firewalls. Packet filter firewalls are limited in their capacity to provide security with functionality, and therefore are regarded as "not very useful". This is not a true statement though. Packet filter firewalls look at every packet both inbound and outbound and check the source address/port and destination address/port against a defined ruleset. Therefore, it is possible to predefine undesirable networks and block traffic coming from them. The packet filter firewall can be an effective noise filter and compliment another more robust firewall solution. Generally they are setup as "allow all except that which is explicitly denied". For example, minimally use a packet filter firewall to filter out:

<u>Incoming</u>
The private IP networks (10.0.0.0; 172.16.0.0; 192.168.0.0)
Loopback network 127.0.0.0
All Broadcasts

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Outgoing
Outgoing ICMP echo reply

Also, it may be beneficial to use all or part of the Internet Storm Center's block list to filter out traffic from hostile networks. Caution is needed as this list changes frequently resulting in a false sense of security, or causing access to be denied to a network the business deems necessary. The block list is located at http://feeds.dshield.org/block.txt
The bottom line is, since routers are a part of every network they should be used to not only route network traffic, but also provide perimeter security to the networks they connect.

Firewall Type 2 – Proxy Server

The proxy server firewall is a hardened server that is running a particular proxy application software such as Sidewinder or Gauntlet. This server mediates the traffic between networks; usually the internal network and the untrusted internet. To the internal client the proxy delivers the responses from the external servers. To the external servers the proxy acts like the client requesting services. This is accomplished by the server tearing the incoming packet completely down, and then checking the contents against the security ruleset. If allowed, it builds the packet with its own IP and MAC address as the source and sends it to the destination address. Because of this function the firewall is performing Network Address Translation (NAT), a common tool used to hide one or more IP addresses behind a single IP address (the external IP address of the firewall in our discussion).

Proxy servers are generally thought to be the most secure firewall; however, that comes with the sacrifice of slower performance, more resource demands, and less flexibility than other types of firewalls. Proxy servers make their gains in that there isn't a direct connection between the internal network and the untrusted external network. They require the client to authenticate to the server, and once this occurs they are able to inspect and apply rulesets throughout the upper layers of the TCP/IP stack. This allows for a more granular ruleset to be applied.

For example: There is a policy against using FTP to post documents on the internet but the retrieval of documents is permitted. The proxy server would tear down the entire packet, inspect it for *put* or *get* commands, and deny all *put* commands while allowing the *get* commands. Without being able to check the entire TCP/IP stack, FTP as a whole would be filtered out instead of the individual subsets.

Proxy servers are typically setup as "deny all except that which is explicitly allowed".

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Firewall Type 3 – Stateful Inspection Firewall

The Stateful Inspection Firewall is the balance between the faster, less secure packet filter and the slower, more secure proxy server. They act with more functionality as a packet filter while they are also capable of seeing into the packet to provide a less robust proxy service. The result is faster throughput and a high degree of security. The most common firewall of this type is Firewall-1 from Checkpoint Software Technologies. Others would include Cisco PIX and IPTABLES in various Linux distributions. As the name implies it inspects each packet and creates a state table of connection information and application information if necessary. Any connection that doesn't match up with information in the state table must then pass the ruleset in order to make it through. The stateful inspection firewall is more robust than the packet filter because it can detect anomalies within the packet such as sequence number errors or incorrect flag options. This benefit provides additional protection against attacks of this nature.

Example Scenario: All inbound traffic is denied. Internal clients are allowed outbound connections to anywhere using http.

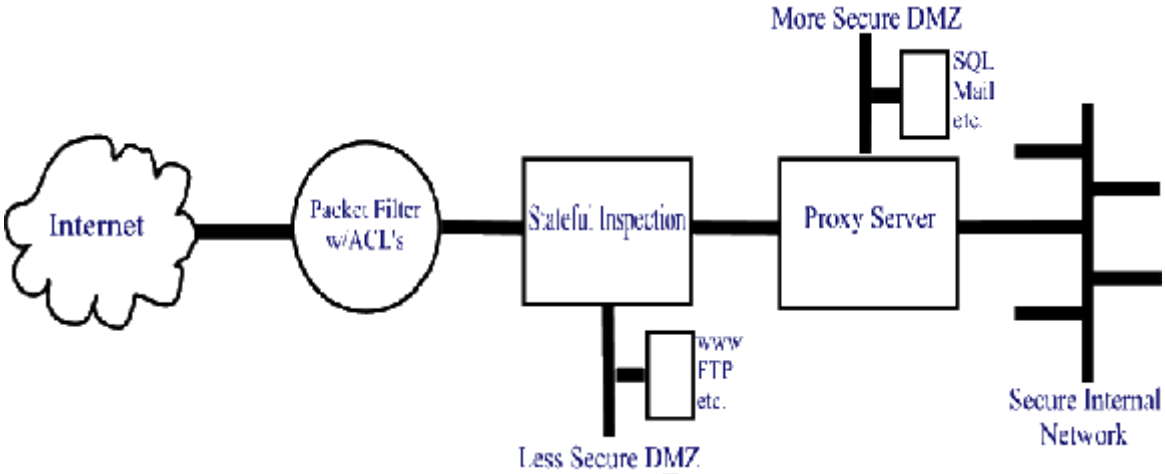
1. Internal Client A requests a connection (SYN) to External Server B
2. Firewall checks the state table then the ruleset and allows the connection while also creating an entry in its state table.
3. External Server B replies to the request (SYN/ACK) back to Client A
4. The firewall receives the packet and checks it against the state table. Since it belongs to an already established connection in the state table the firewall allows it through without matching it to the ruleset.
5. Client A returns an acknowledgment (ACK) to Server B completing the three-way handshake making ready for communications.

Our example, though simple, shows the power of the stateful inspection. Remember all inbound traffic was denied yet we had inbound packets from Server B make it through to Client A. This is because of the state table, without which the ruleset would have denied the packet.

Stateful Inspection Firewalls are typically setup as "deny all except that which is explicitly allowed". Also, all the benefits of Network Address Translation (NAT) are available and should be used as *standard operating procedure*.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Below is a diagram showing a very secure perimeter gateway using all three Firewall types in a way that utilizes each technology to its maximum potential. It was illustrated by Eric Cole at the SANS conference March 2003 in San Diego.



Firewall Summary

Firewalls are an invaluable tool for information security professionals. When deployed properly they can provide a high level of security and functionality. Firewalls should also be used as internal devices as well, to protect critical networks or hosts from employees or business partners. All logging should be turned on and archived for audit and forensic purposes, as well as analysis for intrusion detection.

Firewalls are not perfect. They cannot protect against poor configurations, bad implementations, backdoor network access via modems, viruses, end users, software bugs, etc. This is why they are only one layer of many in our **Defense in Depth** Strategy.

Defense in Depth – Intrusion Detection Systems Layer

A complement to any Firewall strategy is the use of Intrusion Detection Systems. While the Firewall will act as a shield it is not bullet proof. Subject to attacks themselves the firewall cannot protect against end users, modem access, social engineering, poor configurations, etc. To make matters worse, this activity and its effects end up on your network completely unnoticed. Intrusion Detection Systems {Network (NIDS) and Host (HIDS)} monitor and collect activity either on the network or a host. They examine the data to detect threats, attacks, and other malicious activity. This is extremely valuable, because without it you are blind to the activity happening on your network and hosts.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Intrusion detection systems come in basically two flavors, Network based (NIDS) and Host based (HIDS). Separation between the two doesn't mean to use one or the other. Both types should be used to create this layer of defense.

Network based IDS (NIDS)

NIDS are typically hardened systems/appliances, running IDS software, that sit on the wire, monitoring all the network traffic passing by. They do this running in promiscuous mode much like a sniffer. Some common NIDS are RealSecure and Snort. NIDS match network traffic against a database of known or custom attack signatures. A match against the database can be handled in a variety of ways such as a pager alert, email alert, and/or a predetermined course of action.

Some advantages to NIDS are:

- Real time detection
- Neutralize Denial of service attacks and floods
- Detects unsuccessful attacks
- Evidence collection for forensic analysis
- Detect Port Scans and recon
- Fairly easy to setup

Disadvantages to NIDS include:

- Must keep signature database updated regularly
- Difficult to keep up with fast networks (>100Mbs)
- Fooled by encrypted traffic
- Low and Slow attacks
- Switched networks

Switched networks pose a particular problem for NIDS in that they can only see traffic intended for them, or Broadcast type traffic. To get around this, a spanning port can be setup on the switch the NIDS is connected to. If your switch doesn't support it then deployment needs to be strategic. NIDS should be placed before and after your internet gateway, on all DMZ networks, before and after the gateway to any critical internal networks, and in front of any critical hosts.

Host Based IDS (HIDS)

HIDS operate a little different than NIDS in that they watch the server for any activity, determine if there was a security breach, and respond based on criteria setup by the security admin. Some common HIDS are RealSecure Server Sensor and Tripwire. There are different products that take different approaches to Intrusion Detection. Some monitor the log files (Syslog for Unix or System, Event, Security logs for Windows systems) while others check files for changes on scheduled intervals, or both. It is a good practice to start with a hardened uncompromised system to form a baseline for your HIDS.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Some Advantages to HIDS are:

- Monitors specific system activities
- Detects attacks against hosts that NIDS miss
- Is not defeated by encryption
- Requires no additional hardware

Disadvantages to HIDS include:

- Uses system resources
- Not real time
- Difficult to deploy/manage in large environments

HIDS should be deployed on all critical servers including Firewalls, DNS, Email, Web, Servers providing other security functions (content filtering), business critical servers, etc.

Combining NIDS and HIDS is the most effective way to implement an Intrusion Detection defense layer. As the technology unfolds in this area there is a move towards Intrusion Prevention rather than just detection. It would be well worth the time to investigate the upcoming technologies and see how they may fit into your **Defense in Depth** plan.

Defense in Depth – Content Filtering Layer

Content Filtering

Today most businesses require, at a minimum, email and web browsing to effectively communicate with internal, as well as external, customers. While this provides the business with an avenue by which to communicate, it also provides a convenient mechanism for “malware” (i.e. malicious viruses, email, html, etc.) to proliferate and inundate a network, and its systems, in a matter of minutes. In addition, an increase in “Web Surfing for fun” and non-business related email results in higher business costs due to lost productivity. Content Filtering is an excellent way to protect the business by proactively keeping viruses, spam, erroneous web surfing, and inappropriate file attachments to a minimum.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

On the SANS website there is a page titled:
Mistakes People Make that Lead to Security Breaches

Located at http://www.sans.org/resources/mistakes.php

The following are the top two mistakes.

1. Failing to install anti-virus, keep its signatures up to date, and apply it to all files.
2. Opening unsolicited e-mail attachments without verifying their source and checking their content first. Or executing games, screen savers, or other programs from untrusted sources.

(SANS Institute www.sans.org)

As you can see the top two, without any others from the list, are enough to cripple a business. Content Filtering is a defensive measure to use against these mistakes, as well as combating other issues inherent to content.

For our discussion we will focus content filtering primarily on the following areas:

- Antivirus
- Spam
- File Attachments
- Erroneous Web Surfing

Antivirus

It is unthinkable to not have some kind of Antivirus system in place; but too often it is deployed only on the desktop, if at all, and not regularly updated. Antivirus should be deployed in four main places.

- Desktops/Laptops
- File Servers
- Email Servers
- Gateways

Antivirus should also be easy to deploy & configure, unnoticeable, and self-updating. This will help ensure that it can be quickly deployed, users won't try to tamper with it, and it is always current. Since every Antivirus vendor has its pros and cons it is a good practice to use a different vendor for each deployment area in your organization. By doing this you will achieve a greater level of protection against viruses that may slip past a single vendor solution. The following scenario may fit into your organizations Antivirus needs.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Use Vendor A's product, which is very reliable at scanning compressed files, on the desktops.
Use Vendor B's product, which is very reliable at detecting macro viruses, on the file servers.
Use Vendor C's product, which is specialized for the email servers, to protect the email system.
Use Vendor D's product, which is very reliable at detecting Viruses in the Wild, at the gateways.

The idea is, that while each vendor's product can protect in a variety of areas, they most likely specialize in one or two compared to the others. We then take these specialties into consideration and deploy the technology at a particular area for maximum impact.

Spam/Email Attachments

Spam is a problem for everyone with an email address. However, there are a couple of simple cheap things to do to fight off spam before getting into thousands of dollars for big solutions.

1. Implement reverse lookups on the domain of all incoming mail and reject those that do not have an entry.

2. Subscribe to a filter list like SPEWS (www.spews.org). They maintain a list of IP address blocks of known spammers. When incoming mail is compared to the list and there is a match; mail can then be dropped, returned, or simply bounced to SPEWS for an explanation.

These two solutions should cut down, but won't eliminate, the amount of spam received. However, caution should be used especially with solution #2, because you could end up blocking legitimate business required mail from getting through.

The preferred way to combat spam and deal with email attachments is to use a third party SMTP filtering system. There are many products that filter SMTP traffic to stop spam and other unwanted traffic such as unauthorized file attachments. In fact, in our example earlier for Antivirus, the same system to protect the email server may also provide spam protection and attachment checking/stripping via plugins as part of a complete package. Spam protection is handled with a database of known spam signatures that is compared to the incoming mail for a match. When a match is made the system can put the mail into a holding folder, pending admin approval. It can also be dropped or returned.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Attachments can be stripped away based on different criteria; like file size, extension type, recipient address, sender address, etc. At a minimum, unless there is a business need, files with extensions (.vbs .scr .bat .com .exe) should be blocked. Some systems have plugins that boast of being able to detect flesh tones within graphic files to prevent pornographic material from passing through. This is a nice way to add personal protection to the user community. Also, an added bonus with SMTP filtering systems like these is the ability to scan outgoing mail for potential sensitive material that is not authorized for outbound mail.

Erroneous Web Surfing

While many employees follow the rules when it comes to surfing the web during work hours, there are always those who either don't care about the rules or plead ignorance to them. In any case, besides having it spelled out in an acceptable use policy, an HTTP filtering system can and should be installed to limit the sites employees can go to. Probably 99% of businesses out there would not want their employees, with company resources, visiting websites of the following categories: X-rated sites, Job searches, Hacking, Racism, Gambling, Illegal drugs. This can be easily accomplished with an HTTP filtering system.
Surf Control and Websense are the two biggest names for HTTP filtering. Operating with a database of url's that is updated daily, you select the categories to be blocked based on your business needs. Both have many features like setting up quota time for users, blocking by keywords, or deferring to after hours browsing. Also, they have the ability to make allowed and denied lists to override the database, which is useful for special cases.

As you can see, Content Filtering can be an effective part of your **Defense in Depth** plan. Even though many don't include it as **Defense in Depth,** I choose to because of the benefit that comes from it. It provides the user with personal protection against unwanted websites, images, and email. It protects the systems and data by actively scanning for viruses and other malware. It protects the network by filtering out unwanted traffic like spam, and stops worms from spreading. As a result the business as a whole benefits from the protections afforded by Content Filtering.

Defense in Depth – Data Encryption Layer

Data encryption provides the last layer of defense, should an attacker break through the outer layers of your **Defense in Depth** strategy. Encryption sounds familiar to many and the concept is pretty simple. However, all too often encryption is not implemented for various reasons; one of which is people don't understand it beneath the surface. This discussion will be kept at a high level as a defense layer strategy, but I suggest visiting the SANS Reading Room at http://www.sans.org/rr/ for some excellent papers that get deep into the heart of encryption.

Data in Transit

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Encryption of Data in transit is probably the most common form practiced today. In fact, many use it on the internet and may not even realize it occurs. This is utilized to prevent a would-be attacker from sniffing the network for a “Man in the middle attack” or a “Session replay attack”. Typically the data is encrypted when leaving the host and decrypted upon arrival at the client or vice versa. SSL/TLS with a strong encryption algorithm is widely adopted by many vendors for secure Client/Server communications and is the common way secure internet transactions are performed. Also, SSH is a very secure way to perform encrypted FTP sessions.

Stored Data

While encrypting your data in transit is a good practice for protection from network sniffing, it does absolutely nothing to protect the data (typically databases) at its residence. Encrypting only the data in transit breeds a false sense of security because the stored data is more vulnerable as it sits in plain text on a server. Some of the vulnerabilities associated with unencrypted stored data are:

- Theft of the entire system
- Theft of the hard drives
- Theft of the backup tapes
- Console access
- Hacker intrusion through the network

In order to combat these vulnerabilities we use encryption of the stored data so only those with the proper credential(s) (i.e. passwords, tokens, etc.) can be authorized to read the data. At this point any successes in exploiting the above listed vulnerabilities will not produce readable data for the attacker.

There are many different opinions on how to implement Data Encryption. Without belaboring each viewpoint some things to consider are:

- Industry/Business needs - does the industry/business have a standard to which you should comply. (i.e. Healthcare, Government, Law enforcement)
- The performance impact of Data Encryption.
- The cost of the performance impact in dollars.
- Using Operating System level encryption or third party software.
- Encrypt all or just the sensitive portions of the data.
- Seamless integration for end users.

Since there is no guarantee that all of our defenses will stop an attack, encrypting data in transit, as well as the stored data, provides an excellent last stand in the fight to keep its Confidentiality, Integrity and Availability.

Conclusion

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

As you can see, having come this far, we have a daunting task ahead of us. Keep in mind that Rome wasn't built in a day, and neither will your **Defense in Depth** strategy. This will be an ongoing process, and will never really have an end, so don't try to finish it up in a weekend.

Defense in Depth is the most efficient and practical way to build an Information Security Plan, but it is not all there is to information security. **Defense in Depth** is the framework and/or foundation for your Information Security needs. There are many other daily, weekly, monthly, and annual pieces to the security puzzle that go a long way to complimenting a **Defense in Depth** setup. A few to mention are listed below:

- Patch Management
- Vulnerability Scanning
- Penetration Testing
- Password Cracking
- Network Scanning
- System Hardening
- Log Review
- DRP/BCP

We all know perfect security is a myth and cannot be achieved, but with **Defense in Depth** strategies there is much that can be done to minimize risk. Stay the course; we're all in this together.

References

Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal.
SANS Security Essentials with CISSP CBK Volume Two version 2.1.
SANS Press. February 2003.

Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal.
SANS Security Essentials with CISSP CBK Volume One version 2.1.
SANS Press. February 2003.

Einwechter, Nathan. Preventing and Detecting Insider Attacks Using IDS.
March 20, 2002. http://www.securityfocus.com/infocus/1558

Human Error Causes Most Security Breaches. March 19, 2003
http://www.cw360.com/articles/article.asp?liArticleID=120277&liFlavourID=1&sp=1

SANS Institute. Mistakes People Make That Lead To Security Breaches.
October 23, 2001. http://www.sans.org/resources/mistakes.php

Galik, Dan. Captain United States Navy. Defense in Depth: Security for Network Centric Warfare. April 1998. http://www.chips.navy.mil/archives/98_apr/galik.htm

Armstrong, Illena. Policy that lives Enforcing security in spite of the users.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

SCMagazine July 2003. pgs. 30–32

Garfinkel, Simson. Inbox Patrol. CSO Magazine February 2003 pgs. 53-55

Woody, Carol. Internet Content Filtering. January 9, 2002.
http://www.sans.org/rr/paper.php?id=2

Howard, Jeffery. Packet Filters, Stateful Packet Filters, and Proxies.
http://www.burningvoid.com/iaq/firewall-type.html

Paul, Brooke. Building an In Depth Defense. Network Computing. July 9, 2001.
http://www.networkcomputing.com/1214/1214ws1.html

Bace, Rebecca. An introduction to Intrusion Detection and Assessment. ICSA Inc. http://www.icsalabs.com/html/communities/ids/whitepaper/Intrusion1.pdf

Checkpoint Software Technologies LTD. Build Your Security Infrastructure With Best Of Breed Products From OPSEC. 2003
http://www.checkpoint.com/products/downloads/opsec_whitepaper.pdf

SSI Service Strategies inc. Stateful inspection in a Firewall.
http://www.ssimail.com/Stateful.htm

© SANS Institute 2003, Author retains full rights

Last Updated: September 5th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced