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.

Security Lifecycle - Managing the Threat

This paper addresses the security elements that make up a lifecycle, categorized into three areas, Prevention, Detection and Response; what elements are needed to address all aspects of security, how often they should be addressed and how they apply to the overall security posture of the organization.

Copyright SANS Institute
Author Retains Full Rights

AD

Security Lifecycle – Managing the Threat

Mark King

GSEC Practical v1.3

January 14, 2002

Security needs to be addressed as a continued lifecycle to be effective. Daily, there are new attack signatures being developed, viruses and worms being written, natural disasters occurring, changes in the organization workplace taking place and new technologies evolving, these all effect the security posture in the organization. Any one piece of the lifecycle cannot be effective without the other. Identifying risks and correcting them are essential. Perhaps you have a rock solid Information Systems Security Policy, but is that the end? Can you be assured you are secure once you have taken a snapshot and taken actions to fix them? This is a good starting place, but should not end there. The lifecycle needs to be a continued effort for any organization to keep abreast of changes in technology and weaknesses in security that are created as a result of these changes.

It is still surprising how many organizations feel they will never be, or cannot be hacked. CIO and @stake conducted a survey and polled 600 IT professionals who felt their security was good, but in reality were found to have little security, or security not as strong as they thought. You can review the survey results at http://www2.cio.com/research/surveyreport.cfm?id=21[i]

In this paper, the security elements that make up a lifecycle will be discussed; what pieces are needed to address all aspects of security, and how often they should be addressed.

The security elements are categorized into three areas, Prevention, Detection and Response. Each category is discussed below, including what elements fit within these categories and how they address the overall security posture of the organization.

Prevention - How can a company start to think about protecting their company assets without building in some kind of prevention mechanism? Firewalls are designed to protect the perimeter of a network. But just because a Firewall is in place does not mean the network cannot be compromised. Firewalls come in different flavors. They can be a Packet Filter, Application Gateway, Circuit-level or State-full Inspection, and they all are designed to block different types of traffic. It is critical to build in a Firewall rule base that specifies what is and is not allowed to enter into or out of the network. Even with these rules, there is always the possibility of an attack signature that can circumvent the Firewall. For instance, a fragmented packet may be able to pass through a Firewall that does not do State-full inspection. Remember, Firewalls "prevent" the possibility of a compromise by protecting the perimeter.

Another element of Prevention is the assessment. Both the Vulnerability Assessment and Penetration Test address risk levels and "holes" that need to be corrected. Without an assessment, you may never find the weaknesses in the organization's security. The Vulnerability Assessment will address not only Network & Host level risks, but also

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

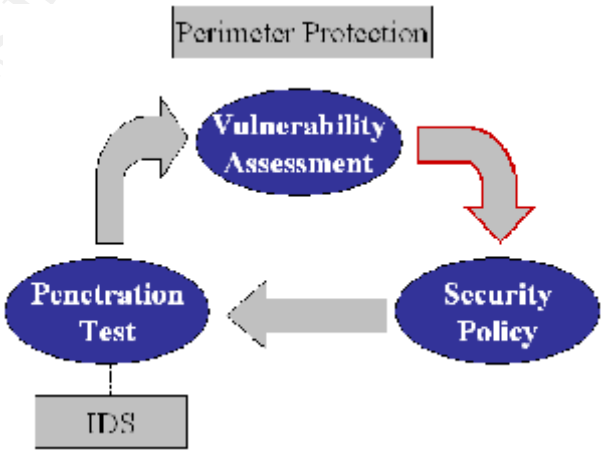
overall security risks within the organization to include Physical, Logical and Data. Penetration Testing is a great way to "test" the security strength once risks have been identified and corrected.

Detection – Intrusion Detection Systems (IDS) and Firewall's both are Detection measures. The IDS monitors the network traffic for attack signatures, and reports any occurrence by risk levels that have been defined. Depending on where the IDS sensor is placed, inside the Firewall or outside the Firewall, it can serve both as "detection" and "prevention". The Firewall itself acts as a detection measure, since all activity is logged and should be reviewed. Assume your Firewall is blocking traffic defined in your rule base, it will write to a log file with all failed and successful attempts. By reviewing the log file, you can determine if someone may be looking for holes in your Firewall by the type of activity that is taking place.

Response – What happens should there be a compromise? Keep in mind, a compromise can not only happen by breaking into the Firewall, but by an internal employee, backdoor access into a network from a modem or even physical entrance to an area by someone pretending to be an authorized person (this is called Social Engineering). The Information Systems Security Policy (IS Security Policy) falls into the "response" category. The IS Security Policy is a written document defining Management's intentions on how Security is addressed. Response can also be handled with Computer Incident Response Team (CIRT) and Computer Forensics experts should an investigation need to be conducted.

Elements of the Lifecycle

- Perimeter Protection
- Risk and Vulnerability Assessment
- Information Systems Security Policies
- Penetration Testing
- Intrusion Detection



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

1. Perimeter Protection

First things first. Firewall, Firewall, Firewall. There is only one way to secure your internal network from a possible external compromise, unplug it! We all know this is not a realistic choice in today's daily operation. Years ago, when the Internet was not such an integral part of today's business world, the only concern of compromise would be from the inside. Now that almost everyone is connected to the Internet, there is a need for some type of protection to be put into place. There are many popular brands of Firewalls available, from freeware applications running on Linux[ii], to commercial Firewall appliances[iii]. You need to determine what type of control your Firewall will be providing. Below are the common types of Firewalls available[iv]; others not mentioned include a hybrid of combining some of these types together.

- Packet Filter – Packet filters are usually part of a router. The router will compare each packet to a set of rules, and depending on the rule, the Firewall can drop the packet or route it to the destination. The rules can include source and destination IP addresses, source and destination port numbers and protocols. The advantage of a Packet Filter Router is the low cost and low performance it puts on the network. The disadvantage is it only works at the Network layer and does not support Network Address Translation (NAT), to hide IP addresses behind the Firewall like the Circuit-based Firewall.

- Application Gateway – This is also referred to as a Proxy server. This type of Firewall is application specific, and works at the application layer of the OSI model. If there is no proxy defined, packets cannot access those services. The advantage of the application level gateway, or Proxy, is it can filter application specific commands like ftp, telnet and http. This cannot be accomplished with other Firewalls that are packet filtering or circuit-level because they do not filter at the application level. The disadvantage is the performance hit on the network, as a result of the context switching that takes place.

- Circuit-Level – Circuit-level Firewalls work at the Session layer of the OSI model, and TCP layer of the TCP/IP model. They monitor the TCP negotiation between packets to verify the requested session is valid. The advantage of Circuit-level Firewalls is they can hide the information about the inside network using Network Address Translation (NAT), making the packet appear to originate from the Firewall. The disadvantage is they do not filter individual packets.

- State-full Inspection –This Firewall combines the three other Firewalls into one. It allows connection between the client and host using multiple layers. It filters packets at the network layer, verifies that packets are valid at the session layer, and evaluates the contents at the application layer. The advantage of State-full inspection Firewalls is they are transparent to the user, offer a high level of security and good performance. The disadvantage of this Firewall is the complexity to administer it.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The Firewall is the first part of securing your infrastructure. It does not make a lot of sense to perform a Vulnerability Assessment without some type of perimeter protection in place. Without a Firewall, your entire network is wide open. But the Firewall is still considered part of the Security Lifecycle, and it should be. After all, once the Firewall is in place, you will at some time or another, add or change a policy rule. Perhaps, you will apply a new version, upgrade, or install patches. Changes to your Firewall will no doubt happen, often! So the Firewall needs to be reviewed and tested to make sure it is still doing what you are intending it to do. Much of this review will be addressed during the Vulnerability Assessment. Perhaps you may decide not to do the Vulnerability Assessment and go right for a Penetration Test. In this case, constant review of the Firewall is necessary to ensure nothing has been left open. Look at your rule sets and log files, review them regularly. This is the only way to be assured you are blocking everything you intend to.

2. Risk and Vulnerability Assessment

This is most often the first step in a security lifecycle. A thorough Vulnerability Assessment will address risk at all levels within an organization to identify the Integrity, Confidentiality and Availability of the organization's assets. We all know there can be a loss of data if our networks are hacked from the outside. What about the inside? In reality there are a high percentage of compromises that have been caused from inside a company's network. For example; internal compromises can be caused from an employee with unrestricted access "playing" or, in the case of a new administrator, learning on the job and configuring software incorrectly, causing a denial-of-service (dos).

But there are many other logical and physical areas that also need to be reviewed during an assessment in addition to the networks and hosts. The following are key areas that should be addressed during an assessment.

- Exterior security – fencing, lighting, building location
- Secured dumpsters – Have you heard of dumpster diving? Yes there are people that will look through company trash looking for confidential information
- Building security – Key locked doors, biometric authentication[v], physical guards, cameras
- Departments - logically broken up, kept secure
- Passwords - post-it stuck under a keyboard or side of the monitor with used ID and password
- Computer/Data Center – environmental controls, fire suppression, cable management, secure consoles
- Data Classification – Confidential, Secret, need to Know
- Access groups – assigned by user and/or group
- Human Resources and IT staff coordination
- Unauthorized modems
- Social Engineering – persons pretending to be an employee, or maintenance worker to gain unauthorized access

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The assessment will itemize all risk levels associated with the areas mentioned above. Should any of these areas become compromised, how will it effect the operation of the organization? Will there be a loss of revenue, loss of reputation, possible lawsuits?

Information generated from the data gathering process will help the IT staff and Management to make logical decisions on how to better protect the company assets. This data will also serve as a reference to creating and/or updating the Information Systems Security Policy.

Network and Host level assessments can be performed using a number of commercial and freeware tools. This paper is not intended to make recommendations on which tools to use, however, there are many good web sites that list several of the popular tools available. SANS publishes a great "Roadmap to Security Tools and Services" poster twice a year that lists many tools by interest area[vi].

3. Information Systems Security Policy

The Information Systems Security Policy is made up of a collection of individual documents called policies. Policies are one of the most critical elements of a proper security plan. Every organization will have a different set of policies depending on the organizational needs. These will define what are and are not accepted practices. The following is a partial list of policies that could be included in an IS Security Policy found on the Pentasafe Security Technologies website http://www.baselinesoft.com/

- Firewalls
- Electronic commerce
- Digital signatures
- Computer viruses
- Encryption
- Contingency planning
- Logging controls
- Internet
- Intranets
- Privacy issues
- Outsourcing security functions
- Computer emergency response teams
- Microcomputers
- Local area networks
- Password selection
- Electronic mail
- Data Classification
- Telecommuting
- Telephone systems
- Portable computers
- User training

Once the policies are developed, everyone within the organization is required to review them, and acknowledge them with a signature. A "written" IS Security Policy is the document that describes Management's intentions from a security perspective. Should there be a compromise, abuse or other violation, Management is protected from possibly being held liable for loss of company assets. Because of the ever-changing environment of most organizations, the Information Systems Security Policy is a document that needs to be reviewed, and modified if necessary, on an annual basis.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

So where do you start in the development of the Information Systems Security Policy? You could hire a Security Consultant to create these Policies for you. Or if you have the resources, these can be done in-house. There are many sites on the Internet that have sample Policies that can be downloaded, but be careful as to how they will apply to your organization. An excellent starting place would be Charles Cressen Wood's book, Security Policies Made Easy, from Pentasafe Security Technologies[vii]. This book is well worth the money, as the author has provided just about every policy you can think of. Choose the policies that apply to your organization, and with a little modification, your policies should be professional and efficient.

4. Penetration Testing

Is this really necessary? Here are a few questions to ask yourself.

- How vulnerable is my technology infrastructure to network attacks from outside the organization?
- By what means can hackers / crackers gain unauthorized access to my technology and information resources?
- Are Firewalls, routers, modems, and other network devices configured correctly and managed correctly?
- How well does my Information Systems Security Policy support access barriers, rights, and privileges to my technology infrastructure?
- How many of my Internet Protocol (IP) addresses are visible/accessible to the "outside world" and what services are available on those addresses?
- How many "modem tones" does my organization present to the "outside world" and how vulnerable are those modems to hackers?

Once a Vulnerability Assessment has been performed and fixes have been applied, the Penetration Test is a good exercise to test how strong the security is from outside the network. This is usually performed as a zero-knowledge brute-force attempt to gain access into the network. Typically, a hacker/cracker will gather information, called profiling, about your operation before they try to launch an attack on your network. If you have the same team that performs the Vulnerability Assessment performing the Penetration Test, you will not be emulating the same results of a hacker/cracker. A security person with zero-knowledge about your organization would best emulate what a hacker/cracker does during the profiling stage. The idea is to use a person that has no knowledge of information that was gathered during the Vulnerability Assessment about the organization. This will result in the same outcome as if someone actually did compromise your network, giving you the information needed to correct the security weaknesses before an actual attempt is made.

5. Intrusion Detection

So you have a locked down, tight Firewall, assessment looks good, a strong written Information Systems Security Policy is in place, and everyone has gone through security awareness training. How do you monitor all those potential compromises, both inside and outside your network? You can review your Firewall logs, and hopefully there are

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

rules in place that are blocking those attempts, and these should be reflected in your log files. But what about those attack signatures that are not defined in a rule? Intrusion Detection Systems (IDS) are designed to monitor all traffic destined for your network, or out of your network. The IDS when configured properly will show all potential attack signatures at different risk levels. When these are noticed, a quick review of the Firewall rule policy will tell you if the source IP's, ports and signatures are being blocked. If not, this is a good time to add them to the rule base. The following are items that an Intrusion Detection System will address.

- Monitors system, event and security logs for a change in files, comparing the new log entry with attack signatures
- Checking key system files and executables via checksums at regular intervals for unexpected changes
- Monitoring of port activity and alerting administrators when specific ports are accessed
- Define type of attack
- Contain the Intrusion
- Identify the source
- Notifies all interested parties
- Review/Repair of systems
- Detailed post-mortem of the Intrusion

There are many choices for Intrusion Detection Systems, most fall into two categories, host-based and network-based.

- Host-based – Host-based IDS are used to monitor the system itself for abuses and internal (system) attacks.
- Network-based – Network-based IDS are used to monitor the network for TCP/IP type of external attacks.

It is important to understand the different type of attack signatures, and how they are used to launch an attack. You can easily determine when some one is ping flooding or port scanning you. But a good hacker/cracker will usually do a series of pinging, probing, DNS gathering, and any number data gathering techniques before an actual attack is launched. A seasoned security person should be able to monitor an Intrusion Detection System, and notice by the events that are taking place if someone is using an off-the shelf port scan utility, or if they are actually gathering pre-attack information. An option to consider is out-sourcing the IDS monitoring to a security company. These companies usually have on staff a good number of very knowledgeable security people that monitor networks in a Network Operation Center (NOC) 24 hours a day, 7 days a week.

Incident Response

Part of the Lifecycle, well, not really. But because Incident Response does fall into the "response" category, it has been included here for informational purposes.

© SANS Institute 2002, Author retains full rights.

When a possible compromised has been identified, proper steps must be followed to initiate an investigation.

- Contain the Intrusion
- Define type of attack
- Identify the source
- Notifies all interested parties
- Engage a Computer Incident Response Team
- If necessary, bring in a Computer Forensics expert

You are not alone, incidents happen all the time. Incident Response Teams and Forensic experts are available to assist in these emergencies. There are a number of Computer Incident Response Teams that go to work to find a solution once an incident has been recognized. The coalition, Forum of Incident Response and Security Teams (FIRST), consists of teams from a wide variety of organizations including educational, commercial, vendor, government and military. Their sole purpose is to respond when new viruses, worms, Trojan's and anything else that causes havoc are discovered. Because FIRST is a coalition, the resources are rather large, giving them a best-defense advantage.

Conclusion

Remember, Security is a LIFE CYCLE. These elements need to be performed on a scheduled basis, at least annually. The following is a re-cap of the cycle in steps.

- Implement perimeter protection using a Firewall, review rule sets and log files regularly
- Perform a Vulnerability Assessment at least once a year
- Develop a written Information Systems Security Policy. Review and update the policy at least once a year
- Test the strength of security by performing a Penetration Test at least once a year
- Monitor all network traffic using an Intrusion Detection System
- Should there be a possible compromise, respond immediately

There is no guarantee that your organization will ever be 100% secure. As an example, take into consideration how a bank would secure its assets; can they be 100% safe from a possible loss? A bank can install state of the art alarm systems, have security cameras throughout the building, install crack proof safes, place security guards on the premises, but should a person really be determined to rob that bank, they probably will. This is also true for Information Security. The best any organization can do, is deter the possible hacker by making it more difficult to gain access.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[i] CIO and @stake "CIO Security Worksheet" results.
URL http://www2.cio.com/research/surveyreport.cfm?id=21 (12 August 2001)

[ii] Configuring a Linux Firewall
URL http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html (26 February 2000)

[iii] List of Commercial Firewalls
URL http://www.icsalabs.com/html/communities/Firewalls/certification/rxvendors/index.shtml
(18 January, 2002)

[iv] William Cheswick and Steven Bellovin, "Firewall and Internet Security"
Addison Wesley, 1995 (although an older publication, well worth the reading)

[v] Biometrics – quick explanation "What is Biometrics?"
URL http://www.antionline.com/fight-back/What_Is_Biometics_And_How_Can_I_Use_It.php
(24 January, 2002)

[vi] SANS "Roadmap to Security Tools and Services" poster URL http://www.sans.org/tools.php
(24 January, 2002)

[vii] Charles Cressen Wood "Security Policies Made Easy" URL http://www.baselinesoft.com/
(22 January, 2002)

L. Taylor, "The Whys and Hows of a Security Vulnerability Assessment"
URL http://www.intranetjournal.com/articles/200010/se_10_18_00a.html (24 January, 2002)

Paul Innella and Oba McMillan, "An Introduction to Intrusion Detection Systems"
URL http://www.securityfocus.com/cgi-bin/infocus.pl?id=1520 (6 December 2001)

Forum of Incident Response and Security Teams
URL http://www.first.org/ (02 January, 2002)

Illena Armstrong, "Minding the Store, detecting rising intrusions"
SC Magazine (November 2000) pg. 36

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced