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.

Outline for a Successful Security Program

Do you need a Security Program? As technology advances, companies are finding out they require a network security program. This paper is meant to give the reader an outline and high level view of security topics to examine when creating a network security program. This paper is broken into fifteen sections related to security. It has been my experience that most security programs will have to give some attention to each of these sections in order to be successful. Some of the topics I will discuss include: security pol...

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia
Stay Secure

Outline for a Successful Security Program

Executive Summary

Do you need a Security Program? As technology advances, companies are finding out they require a network security program. This paper is meant to give the reader an outline and high level view of security topics to examine when creating a network security program.

This paper is broken into fifteen sections related to security. It has been my experience that most security programs will have to give some attention to each of these sections in order to be successful. Some of the topics I will discuss include: security policies, firewalls, intrusion detection systems, documentation and disaster recovery. Explaining each of these topics in great detail is beyond the scope of this paper. You can find more in-depth papers on any of these sections in the Sans reading room located at http://www.sans.org/rr. Every security program is different, so there is no definite order in which these sections should be addressed. However, I will try to start with the topics that are usually dealt with in the beginning stages of many security programs.

Security Policy:

Security policies are arguably the most important aspect of any security program. The question I hear most often is "Why do we need security policies?" There are many answers to this question. Security policies are the heart of your security program. Everything that you do in your security program should be based on or built around your security policies. These policies are a way for a company to define where it stands on security issues. If written and communicated correctly, security policies tell all employees within a company what is acceptable conduct in the work environment.

Many people get confused about the difference between policies and procedures. Hierarchically, policies should be at the highest view; by this, I mean they should be more general than procedures. Well-written policies should be short and to the point. No security policy needs to be more than ten pages in length. The function of procedures is to explain how to follow what is stated in the policy. Sans offers a great place to find more information on security policy at http://www.sans.org/resources/policies/. Writing security policy can be a very time consuming task. Some of you may not have the time to write new or modify pre-existing policies. For those of you who fall into these categories, a book called SOS/RUsecure Information Security Policies may be a helpful resource This book offers hundreds of sample policies that the advanced or novice security professional can use to customize their own policies. It is available at http://www.network-and-it-security-policies.com/policies.htm.

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

Security Awareness Program:

Security awareness is becoming an increasingly important component of security programs. I would not consider any company that does not have a security awareness program to be secure. Employees are the first line of defense against intruders. I am going to tell a story that might have been prevented if this company had a security awareness program.

> A large financial company spent thousands of dollars on firewalls and intrusion detection systems. This company hired a new secretary who had basic access to the network. One day the new secretary got a call from someone pretending to be a new member of the IT department who needed her password to fix a problem with her account. Since the secretary was not aware of what social engineering is, she gave her password to the attacker. Then this attacker was able to log into the network as a user, and find an exploit that gave them administrative privileges.

Had this secretary known that social engineering is when attackers use whatever means necessary to gather sensitive company information, she might not have given out her password. The point I am trying to make is that if employees are not aware of security, many unfortunate things can happen.

One of the main focuses of a security awareness program is to get the employees involved in securing the network. One of the hardest things to do is to impress upon them that network security is everyone's responsibility. There are many things you can do to get help from your employees. One strategy is to make the program as fun and exciting as possible. Mark Desman wrote a great book called Building an Information Security Awareness Program that can provide you with lots of information on how to implement a security awareness program. If you plan to implement one of these programs, it is a must read!

Security training for security staff and network administrators:

"Computer Security is a 40-year-old discipline; every year there is new research, new technologies, new products, even new laws. And every year things get worse." –Bruce Schneier, CIO of Counterpane Internet Security Inc. As companies start to realize how important security is, they may assign or hire a single person to act as their security analyst. As the program evolves and this person is pulling their hair out, management soon realizes that security is a bigger job than originally perceived. If you are lucky, you work on a security team where a few of you share the responsibility. Unfortunately, many of us are going at it alone.

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

Regardless of who is taking care of your company's security, those people need to keep up with the industry. The security field changes in a matter of minutes. There are always new technologies, new security holes and new types of attacks. A network that was secure a month ago might not be secure today. Security training for your security team and your network administrators is important; after all, they are the ones who are trying to protect your data from intruders. Here are the websites of a few highly recommended organizations that provide security training: www.sans.org, www.giac.org, www.cert.org, and www.isc2.org. You can find a great deal of information on security training at any of these sites.

Management Buy-in:

One of the most challenging tasks for security professionals is getting management buy-in for the security program. Management buy-in is crucial to having an effective program. If you can't get management to back your program with support and financing, then your job may be extremely difficult. One reason buy-in can be difficult to get is that many managers do not see through technological eyes - they only understand things from a business perspective.

There are three measurements you can use to show managers the need for security and how it aligns with business in a way that they will understand. These three measurements are business risk, return on investment and total cost of ownership. First you want to be able to show business risk. Which of our assets are under threat and what are those threats? Showing management where the company is at risk is the easiest way to draw attention to the security program.

Figuring out the return on investment is probably the hardest of the three to show. To accomplish this you need to be able to compare the cost you currently spend to solve a problem or protect yourself from a threat and compare that to what it would cost with a new or better technology. When presenting these numbers, you would want to show how the return on investment will secure the company from its risk.

A common mistake that many security professionals make is to underestimate the total cost of ownership for new technologies. A great example of this is if a security professional asks for a fifty thousand dollar budget for a new intrusion detection system. The price that was estimated includes the software; hardware and licensing of the product, but what they forgot to include was the added cost to hire someone to help implement the product. Training will also be needed for both employees, which now put them over the allowed budget and raised the total cost of ownership.

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

If your company does not have security as one of their top issues, you should create a presentation explaining why they should. Getting senior management behind you makes a huge difference when trying to get your users involved in the program.

Disaster Recovery:

A disaster recovery plan is the most important part of every security program that you will hopefully never need to use – except for testing of course. A disaster recovery plan, also known as a business continuity plan, can be defined as a set of steps a company will take to get their business up and running in the event of a disaster. One thing I will say about a disaster recovery plan is that if you don't have one, create one. The simple goal of your disaster recovery plan is to get your company's critical systems fixed as quickly as possible following a disaster. In today's world, time is money. The faster your systems are up after a disaster, the more money your company will save.

Disaster recovery is more than an IT function; it is something that the whole business should be involved in. Your first task is to select members for the team. Team members should be chosen carefully. You want your team members to be quick thinkers, responsible, and knowledgeable about your organization's systems. After you get your team together, you must write the actual plan. There are many resources available to help you. One of my favorites is the "Disaster Recovery Journal". You can find information about disaster recovery events, tools and the Journal itself at http://www.drj.com. Registration is required to view the journal, but it is free if you are responsible for your company's disaster recovery.

A couple of topics that are usually referenced in the plan are backups and communication. How is your company backing up its data, and how do you restore it after a disaster? Also, who is responsible for contacting all the disaster recovery team members and management when a disaster strikes?

Here are four tips regarding disaster recovery:

- Always plan for the worst
- Make your plan into an easy to follow written document
- Talk to your vendors about backup hardware
- Pack a disaster recovery tool bag

Always plan for the worst; it is better to be overly ready than to get caught off-guard. Have your plan in an easy-to-follow order, written down and readily available. The availability of an easy-to-follow detailed list may prevent your team from making many mistakes due to the stress experienced during these high-pressure disaster situations. It is also important to consider how long it

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

would take you to order and receive servers if you lost all of yours in a disaster. Discuss possible disaster scenarios and you resultant company needs with your vendors. Most vendors will make agreements that guarantee new server delivery in as short as a few hours. This will cost a pretty penny, but isn't it worth it to save your company from going under? If your vendor will not do this, you might want to look for one that will. Finally, gather a bag of tools you might need in a disaster situation like cables, hubs, wire cutters and software to name a few. Make sure this bag is only used in disaster situations and restocked afterwards.

Auditing your Systems:

Just about every hardware or software device in the computer world can create some sort of log. Many security professionals do not use this feature to its fullest potential. They take the time to set up auditing, but never examine the logs. One reason for this is because viewing audit logs can be tedious. It is imperative to examine your audit logs; these logs allow you to learn a lot of important information about your systems

There are two ways to setup your auditing. You can either audit everything or customize what you will and will not audit on your systems. By auditing everything, you make sure to get all events. Unfortunately this takes up a lot of disk space and can create so much information that it can be difficult to sort through it all. On the other hand, you could choose to only audit the events you are interested in. This can be much easier to administer, but allows the possibility of important events passing by unnoticed. Your decision on what to audit should depend on your acceptable level of risk.

Auditing has many uses in computer security. In his paper called "Audit Trails", Rajeev Gopalakrishna states that ,

> "Individual accountability is the ability of an event to be traced back to who caused it. Reconstructing events means using the events to figure out what happened. Problem or resource monitoring can help you determine problems like outages and disk failures as they occur. Auditing also plays an important role in intrusion detection."

I believe that the best way to audit is to audit everything, and sort through it all. Disk storage is much cheaper today than it used to be. There are also many log reduction tools that will help sort out only the events you are interested in from the entire logs. Kiwi Enterprises offers a log reduction program like this called "Kiwi Syslog Daemon" that uses the syslog protocol, allowing you to forward, display and log specific events. You can find this tool at www.kiwisyslog.com. If you decide to use any of these types of tools, make sure you backup the log files before using the tools. Monitoring of your network activity will be discussed in a later section.

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

Physical Security:

Physical Security is one area of a security program that is often overlooked. Companies spend thousands of dollars on server equipment and methods of preventing intruders from stealing data through the Internet, and then allow anyone to walk in and sit at the server consoles. Ideally all of your servers should be located in a locked environmentally-controlled room. Companies are now taking better precautions for securing their servers and network hardware. A well designed server room should have access control restrictions. Only the people who need to be in the server room should have access to it. There should be humidity control and temperature control in the room, as well as protection systems for smoke, fire and water. Since server rooms tend to house critical equipment, backup power is often provided by a generator allowing your equipment to stay running in a power outage.

There are a several ways you can control access to your server room. Some companies choose to use the old-fashioned key system. Everyone who needs access is given a key to the room. This method has a few drawbacks. Keys can be lost or stolen creating the opportunity for unauthorized people to gain access to the room. Disgruntled employees could make copies of the key for future use. An electronic badge system could be used to help solve the problem of copies being made for future use; but, if the badges were stolen they could still be used by someone who is not authorized. When building our server room, I chose to use a combination of badges and a numeric access key code. The only people who know the code are those who need access to the room. Nobody but me is allowed to distribute the code. The random six digit code is changed on a quarterly basis, or whenever an employee who knows the code leaves the company. This method is fairly secure, although it is not one hundred percent foolproof. Someone could still give the code and their badge to someone else. Fortunately, the badge system helps to deter this from happening because using the badge creates logs of who enters the server room and at what times.

Biometrics is another technology that can be used to control access. Biometrics is the process of allowing access by interpreting a person's physical traits. Examples of biometrics include retina scans, fingerprints and voice recognition. The secret to why this is the most secure method is because every person will be unique. Nobody's eyes, fingerprints or voices are the same as anyone else's. Biometrics is still a young technology that requires improvement before becoming the standard. I feel that it will become the way of the future for controlling access. Although it is becoming increasingly more popular, biometrics is still a very expensive technology compared to other methods.

Physical security allows you to control who has access your systems. What you use for your physical security will once again depend on your

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

acceptable risk and security budget. If you would like to learn more about physical security, there is a great resource paper written by Justin Bois available at http://www.sans.org/rr/physical/protect.php.

System Hardening:

What is system hardening? According to Al Aric, consultant for alaricsecurity.com, system hardening is "the process of taking an operating system and the applications that are intended to be hosted on the computer and properly installing and configuring them to meet stringent security needs." Your servers will usually be the main target for intruders, but it is still important to tighten the security on your workstations as well. There are three main parts to a system hardening strategy: removal or restriction of vulnerable or unnecessary services, patching security holes and securing access controls.

What services you restrict will depend on what functions your system provides and what platforms you are running. Any server that has direct access to the Internet like a web server should be configured very carefully. It is not always the best idea to remove a service from a system. Reinstalling a service after is has been removed is much more difficult than just re-enabling it. If you might have a need for a service in the future, you will want to disable the service so it can be re-enabled if necessary.

Patch management is one of the most difficult administrative tasks for security professionals. New vulnerabilities are found every day. Keeping all of your systems up to date on patches and hot fixes can take much time and effort, especially if you are working with thousands of clients and servers. Applying the patches is only part of the patch management process; you also have to determine which patches are needed and test them. The best thing to do is to test all the patches before you apply them to your production systems. Many times these fixes are created in a hurry and can contain bugs. There are many solutions for managing this task, including some built in and many third party applications. Some of the third party vendors thoroughly test the fixes for you, which can be beneficial if you have the extra budget.

The last area I will discuss regarding system hardening is access control. The default access restrictions are way to loose for a secure network. For instance, in Windows 2000 the "everyone" group is given too many privileges by default. Here you want to make sure you follow the principle of least privilege. This principle involves restricting access for users, groups and applications to only those they require to perform their job. Security templates, which are template files that can be applied to systems to automatically fix security holes, are worth their weight in gold when used to harden systems, take advantage of them.

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

System hardening may appear to be of relatively little importance when compared to building firewalls and monitoring intrusion detection systems, but don't be fooled. Tightening the systems in your network will greatly reduce the chance of a user or administrator intentionally or unintentionally damaging them. This task also removes many of the vulnerabilities that are commonly exploited by intruders, often sending them on their way to hack someone with weaker security.

Firewalls:

Firewall technology is possibly the most talked about security topic. If you are a security professional, you will have to become familiar with firewalls at some point in your career. A firewall is a system or set of systems that control access between your internal network and some other external network (usually the Internet) according to a security policy. It is basically a gateway to your network that lets you control who comes in and out. A firewall should be a physical representation of your security policy. If your policy says that you do not allow any FTP traffic into your network, the firewall is where you would block this.

There are two types of firewalls, hardware and software. Many people disagree on which type of firewall is more secure. There are many firewall products to choose from if you want to purchase one, or you can build your own. The option you choose will depend on how much your company is willing to spend and how much knowledge and resources you have to dedicate to building your own. Hardware firewalls are network appliances like routers. Linksys and Cisco Pix are a couple examples of these types of firewalls. Most of the research I have done shows hardware firewalls to be more secure than software. Cisco Pix is the only firewall product that I have worked with, and have been very pleased with the results. The following link provides you with some of the features a Cisco Pix firewall has to offer http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm. Software firewalls sit on top of a machine and require an operating system to run off of. Checkpoint offers a popular software firewall. You can find information on checkpoint products at http://www.checkpoint.com/products/protect/firewall-1.html

Now that I have explained to you what a firewall is, I would like to tell you what it is not. **Firewalls are not an overall security solution**. I have highlighted this because it is one of the biggest mistakes management makes. Once a firewall is in place, management often thinks they are safe and sound. Part of your job will be to show management that a firewall is only part of the solution. Firewalls can not protect you against back-doors, social engineering or removable media. Certain firewalls can provide some security against viruses, although if your company has the need for virus protection, you would be better

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

off not solely relying on your firewall for this. It would be beneficial to look into getting an enterprise antivirus software solution.

Although a firewall can provide many functional advantages to your security I am only going to talk about one. There are far too many advantages and disadvantages for firewalls to explain them all here. One of the biggest advantages of a firewall is that it acts as a choke point to your network. Outside or exterior routers in a network are sometimes referred to as choke routers. What this means is that all traffic coming in and out of your network must go through this point. This is provided you do not make available any ways to get around the firewall. Because they are a choke point, firewalls are a logical place to monitor the traffic on your network. If you have a firewall, take advantage of your firewall logs by reviewing them on a regular basis. Checking these logs will help you figure out what is usual and unusual about your traffic.

There are many types of firewall configurations to choose from. All firewalls are different and so are the needs your company has for implementing one. Imy professional opinion, based on my experience and readings, I believe that if you have any business critical information that needs to be secured, and you allow Internet access to your users, the minimum of a screened subnet architecture should be implemented. Figure 6-4 below from O'reillys Building Internet Firewalls 2nd Edition, shows an example of this architecture. This configuration provides added security by using two routers, creating a demilitarized zone or DMZ. In the figure below, the DMZ is referred to as the perimeter network. If the first router gets compromised, there is still another block in place to protect your internal network.

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

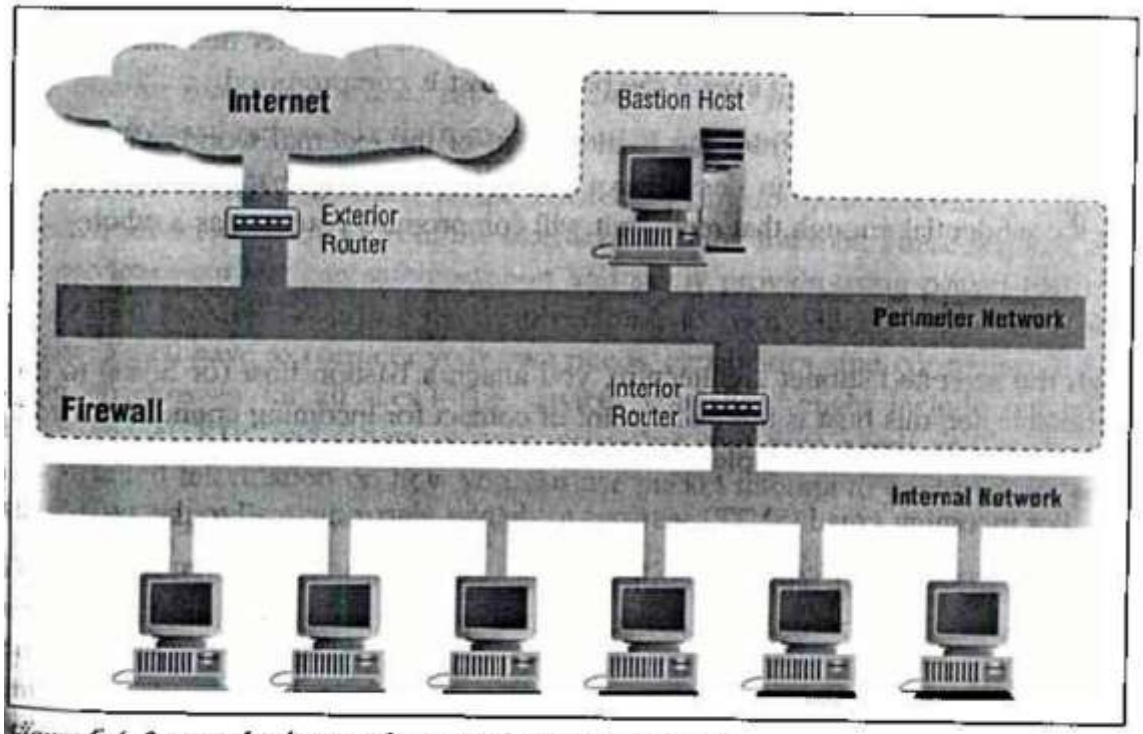

Figure 6-4. Screened subnet architecture (using two routers)

(O'reilly, 2000)

Antivirus Software:

Viruses have been a problem in the computer industry for many years. I am assuming in my writing that if you are reading this, you already know what a virus is. However, if you would like to know more about viruses, then check out www.howstuffworks.com/virus.html. With that being said, I will not go into what a virus is, but give you some of my thoughts on antivirus software. It is unlikely you will join any company with a computer network that does not have antivirus software. With the high number of viruses reported each year, it is an essential part of business. Antivirus software helps to prevent viruses from infecting your systems as well as detecting them.

Antivirus software is one area of your security program where your company would benefit by allocating some funding to. Although there are some adequate free antivirus solutions for personal use, I recommend going with a more popular commercial solution for business. The two most popular antivirus products are Norton Antivirus (www.norton.com) and McAfee Antivirus (www.mcafee.com). It is much cheaper to protect against viruses than to fix the problems they can cause. These next tips will help you with your antivirus solution:

- Reduce network traffic and administration time by using centrally managed antivirus software.

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

- Sign up for many virus alert lists and forums.
- Educate your users on what to do with email attachments.
- Update your virus definitions often.

If you use these tips, you will be well on your way to protecting your network from viruses.

Vulnerability Scanning and Penetration tests:

The best way for you to protect your network, is to test it by trying to attack it yourself. The most dangerous vulnerability is the one you aren't aware of. By running penetration tests and vulnerability scans on your network you can find many of your security holes. Once you have this list of vulnerabilities, you should close the holes that will not drastically affect your business. Vulnerability scanning is really just part of penetration testing. You could consider it to be the reconnaissance for your penetration test.

Vulnerability scanning is the process of identifying vulnerabilities of computer systems in a network in order to determine if and where a system can be exploited or threatened. Whichever vulnerability scanning tools you choose to use whether commercial or free, make sure they are kept up to date with the latest vulnerabilities. The following list is some of the well known scanners out there, but there are hundreds more to choose from:

Free:
- SARA - http://www.ists.dartmouth.edu/IRIA/top_ten/sara.htm
- NESSUS - http://www.nessus.org/download.html

Commercial:
- ISS Internet Scanner - http://www.iss.net
- Symantec NetRecon - http://www.symantec.com/

The first question that will have to be answered is whether to test in-house or have a consultant test for you. If your company has the staff and know how, then do it yourself. By performing these tests yourself, you will learn more about your network. However, in most cases, you will receive better results by having a third party run the tests. Our company chose to have a consultant run the penetration test the first time with me observing. Not only did we get detailed professional results, but I also learned what to do for future tests. It is necessary to run future tests because new vulnerabilities are discovered every week. The following chart found at www.cert.org/stats/cert_stats.html shows the number of reported vulnerabilities from 1995 to the first quarter of 2003. With the total number and rate of vulnerabilities growing every year, you should run at least one penetration test annually.

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

Penetration testing will produce a list or report of all vulnerabilities that were found. Thorough tests should cover social engineering and physical security as well as network security. If you decide to run your penetration tests yourself, I recommend downloading the "Open Source Security Testing Methodology Manual" by Pete Herzog from http://www.isecom.org/projects/osstmm.htm. This document provides a wealth of information on penetration testing. There are three ways you can go about running these tests. You can act like an intruder that has no knowledge of your organization, an intruder that has some knowledge, or like an employee that has limited access. A good place to start is to look on the Internet and find out as much about your company as you can. This is usually the first thing a determined attacker will do.

Passwords, User Rights and Privileges:

I would like to stress the principle of least privilege again. I have referred to this principle a one other time in this paper because of how important it is. User rights and privileges are what you will use to control what your employees can and can not do. It is always better to add rights for someone later if determined that they require them, than to give them more than they require.

Just about all users today are given a home folder in which to save their data. You want to make sure that each person can only see their own data and any public data they need access to. At a minimum you want to separate home folders, HR, payroll and any other critical data from non-critical data. Depending on the security you require, encryption can be used to provide additional security.

Administrators should also be restricted. Too many companies have a group of administrators that all have access to everything. Many administrators even share an administrative account. By sharing an administrative account, nobody can tell which administrator made changes to the systems. Delegated administration is giving your administrators the rights to do some administrative tasks, but not all, and being able to tell who did what. It is a good idea for each administrator on your staff to have their own user and administrative account. Of course, the administrative account should only be used when necessary.

Now, let us talk about the wonderful world of passwords. You can save yourself many headaches by getting management to approve and enforce a password policy. Password problems take up a large majority of helpdesk issues. To administrators, passwords are a very important part of security, but to users, they are an obstacle preventing them from getting their work finished. The first four months of my company's security awareness program was spent educating our users on why we need secure passwords, and how to create them. As an administrator you want to enforce password history, require frequent changes, set a minimum password length, check for complexity requirements

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

and use account lockouts. Most computer systems give you the ability to use these features. The following is a list of password do's and don'ts. It is a good idea to make a list similar to this one and distribute it to your users.

Do's

- Use letters, numbers and special characters
- Use both lower and uppercase
- Change passwords often
- Make passwords you will remember
- Use passwords that are difficult to guess
- Use patterns or sentences

Don'ts

- Use simple keystroke combinations like "12345678"
- Use dictionary words, family names, birthdates or your username
- Write your passwords on notes or store in electronic format
- Give your password to anyone
- Use the same password for all personal and professional accounts

It is important to keep passwords and access to your systems strong and private. If someone gets one of your user's passwords, they can bypass many of the security layers in your defense.

Intrusion Detection Systems:

Intrusion Detection is an expensive technology. You need to do your homework when searching for an intrusion detection system to fit your needs. I am just starting to learn this technology myself. Much of the information I will give you is from my recent research. To get a good overview of the technology as a whole and the difference between host-based versus network-based detection systems, download the whitepaper called "Network-vs. Host-based Intrusion Detection" at http://documents.iss.net/whitepapers/nvh_ids.pdf

The three main aspects for intrusion detection are choosing between host and network-based systems, where to put your sensors, and filter creation. One frequently asked question is "Should I get host-based or network-based systems?" The answer to that question is both! Both types of systems compliment each other by being able to detect attacks the other can't. In many cases, it may be too expensive to support both systems. In this case a network-based system is the better option.

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

The host-based versus network-based problem can be compared to the firewall scenario of hardware versus software. Host-based systems, much like software firewalls require a secure operating system to exist on. Network-based systems, like hardware firewalls are independent of this. Network systems analyze data packets allowing the review of the data to be near real-time. This allows for faster response time to possible attacks. Host systems on the other hand review audit logs. Using filters and notifications can improve the time it takes to spot possible attacks for both types of systems.

Another common argument regarding intrusion detecting systems is whether it is better to place your sensors inside or outside your firewall. The obvious answer once again is both if you have the ability to. By placing the sensor outside the firewall, you can monitor the traffic coming into your firewall. This configuration also allows you to see the pre-attack scans that would otherwise be blocked by your firewall and not seen by a sensor on the inside. Having the sensor on the inside the firewall allows you to see all of the traffic leaving your network. Two benefits this configuration provides are helping you to see if your firewall is working correctly and alerting you if an intruder has managed to get through the firewall.

The architecture I am considering for recommendation will use both network and host-based systems. I will place one sensor outside the firewall and one just inside. All the critical systems on the network (i.e. web servers) will have a host-based system on them. All alerts and information will go to a single central database that can be accessed by an easy to use console. I recommend taking the extra time to create solid filters, so analyzing the logs will be more efficient. Much of the information in this section came from the afore-mentioned white paper and Network Intrusion Detection Third Edition written by Stephen Northcutt and Judy Novak. (2003)

Backup Solutions:

No security program would be complete without having a backup solution in place. Data is one of your company's most critical assets. All the previous sections in this paper have been related to protecting your data. If the other parts of your security defense fail, what will you fall back on? If you have good backups, you will have a place to start over from in the case of a disaster.

Redundancy and accessibility are important when dealing with backups. You want to have redundant backups easily available. Make sure you have them in more than one physical location. What good will your backups be if they are in the same place as your data and the whole building they are in burns down? Your ultimate goal should be to enable your users to access their data twenty four hours a day, seven days a week. This would be considered one-hundred percent accessibility. Even if this is not possible, you want your backups to be

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

immediately available if you need to restore some files that were lost or corrupted.

In this section, I will briefly explain four technologies available for backup solutions. When deciding which route to take, remember that you can combine these options to provide your total backup solution. Before I get into the technologies, I must mention backup procedures. You should have written procedures explaining exactly how to restore your data from backup. These are usually found in your emergency preparedness or disaster recovery plan. It is also important to periodically test these procedures to verify that they work.

The four technologies I will describe are:

- SAN (Storage Area Networks)
- NAS (Network Attached Storage)
- RAID (Redundant Array of Inexpensive Disks)
- Tape Backup

Storage area networks are a collection of networked storage devices that are able to communicate with each other automatically. A SAN is actually a network of its own that is separate of your LAN, usually connected via a fiber connection.

NAS systems are similar to storage attached networks. One main difference between SAN and NAS systems is that network attached storage is actually part of your network. There is currently a huge debate in the industry over which technology is better. There is an excellent paper written by Curtis Preston discussing the ten determining factors in deciding one option over the other at http://www.onlamp.com/lpt/a/1625.

Servers usually come with RAID capability in them. Every server we have on our network has some implementation of RAID. One way to describe RAID technology is that is allows you to take multiple hard disks and use them as one. An example of how all these technologies can be used together is that many NAS and SAN solutions contain servers that use RAID technology.

Tape backup is probably the most common backup solution used today. Data is saved onto a removable media, usually tapes which can then be locked away for safe keeping. If you are using the backup tape solution, you should keep tapes both onsite and off, and store them in a fireproof safe if possible.

I have only scratched the surface of explaining these backup technologies. Before you choose which works best for your situation, you should do some more research on each option. For example, it would be beneficial to examine the added benefits you would receive from a SAN in addition to tape backups to see if it would be worth the extra money for your company.

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

Security Documentation:

This section really pertains to all areas of business. I waited to discuss this section until last, but documentation is something you will work on from day one. Security documentation is used to set clear directions and goals for your security program. There will be lots of documentation from all the security measures previously discussed in this paper.

Take your time when creating your documentation. Provide detailed descriptions of all your security projects, including charts and statistics. These documents can be used to your advantage when showing management where the security budget went. Efficient documentation has many benefits in the computer world. The following is an example of why managers like employees who document well.

> John is the security administrator for Acme Inc. He oversees all areas of the security program in the company. John thinks security documentation is a waste of time, after all he knows his job well and all decisions on security go through him. One day John gets an offer from another company that is willing to pay him a lot more than Acme can afford. John is happy and would prefer to stay with Acme, and asks them to match the offer. When John is denied, he becomes bitter and decides to take the other offer immediately, leaving Acme without divulging any security information. Since there is no documentation or anyone left to train a new security professional, the company will had to spend a lot of time and money to figure out the security of their systems.

If the Acme Company had required John to have proper documentation, the business would not have been affected so drastically when John left.

Another benefit of documentation is that you will learn more about your systems while creating it. You may also be able to see possible holes or weaknesses in your security program when it is laid out in front of you. Document problems you run into or mistakes you made, so that you do not repeat them. The following is a list of documents you will most likely have from your security program. This list is by no means exhaustive.

- Audit logs
- Security Policies and Procedures
- Helpful Tips and Instructions for being a secure employee
- Network Diagrams including: IP numbers, subnet masks, default gateways etc.
- Server Specifications like: operating systems, patch levels, functions etc.

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

- Access and privilege reports
- Vulnerability scans
- User lists
- Risk analysis reports
- Inventories
- Security tool manuals and white papers
- Server change logs (I keep a log of every change or modification that takes place on our servers from installation on)

Conclusion:

I hope this paper has helped you whether you are about to begin a new security program or you are already in the middle of one. The fifteen sections I discussed are all integral parts of security. Exploring these areas should give you a good base for creating a plan to secure your company. Computer technology is always changing. Our society is starting to demand that we have the ability to do everything immediately. Web applications, electronic commerce and the Internet allow us to provide real time services with great functionality. This creates the need for more advanced security.

If you made it this far, you must have interest in the security field. Writing this paper has helped me realize that security is a team effort. As we work together in this industry, our networks become more secure every day. I have always thought that if you can't think of a better way to say something, then borrow it from someone else. So I leave you with this humorous quote about security, "The only truly secure computer is one buried in concrete, with the power turned off and the network cable cut." -unknown

References

Bois, Justin. Apr. 2002. "Protect Yourself" Sans Reading Room.

http://www.sans.org/rr/physical/protect.php.

Conry-Murray, Andrew. "To get dollars they need, security administrators have to start speaking the language of business". Network Magazine. Mar. 2003. Pg 44-49.

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

Desman, Mark B. Building an Information Security Awareness Program. Boca Raton: Auerbach. 2002.

Edmead, Mark T. Ed. Disaster Recovery and Business Continuity Step-by-Step. Sans. 2003.

Gopalakrishna, Rajeev. Apr. 2003. "Audit Trails". The Center for Education and Research in Information Assurance and Security. http://www.cerias.purdue.edu/homes/rgk/at.html.

Herzog, Pete. 26 Feb. 2002. "Open-Source Security Testing Methodology Manual". 3 Jun. 2003. http://www.isecom.org/projects/osstmm.htm.

Northcutt, Stephen and Judy Novak. Network Intrusion Detection Third Edition. Indiana: New Riders Publishing. 2003.

Preston, W. Curtis. 14 Mar. 2002. "The Top 10 SANs vs NAS Decision Factors." 6 Jun. 2003. http://www.onlamp.com/pub/a/onlamp/2002/03/14/sansnas.html.

Roamer. 5 Jan. 2001. Network IDS Sensor Placement. 17 Jun. 2003. http://www.securitytribe.com/whitepapers/IDSplace.html.

Zwicky, Elizabeth D., Cooper, Simon and Brent Chapman. Building Internet Firewalls Second Edition. Sepastopol: O'Rielly. 2000.

"Cert/CC Statistics 1998 – 2003". 16 Apr. 2003. Cert Coordination Center. 5 May 2003. http://www.cert.org/stats/cert_stats.html.

"Network-vs. Host-based Intrusion Detection". 2 Oct. 1998. Internet Security Systems. http://documents.iss.net/whitepapers/nvh_ids.pdf.

"Penetration Testing Guide". 2003. Corsaire Limited. http://www.penetration-testing.com/penetration-testing-guide.html.

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

"Disaster Recovery Journal". 1987. Disaster Recovery Journal Online. 10 May 2003. http://www.drj.com.

Sans .org. 2002-2003. The Sans Institute. 29 Jun. 2003. http://www.sans.org.

Web Links

http://www.network-and-it-security-policies.com/policies.htm

http://www.giac.org

http://www.cert.org

http://www.isc2.org

http://www.kiwisyslog.com

http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm

http://www.checkpoint.com/products/protect/firewall-1.html

www.howstuffworks.com/virus.html

www.norton.com

www.mcafee.com

http://www.ists.dartmouth.edu/IRIA/top_ten/sara.htm

http://www.nessus.org/download.html

http://www.iss.net

http://www.symantec.com/

© SANS Institute 2003, Author retains full rights

Last Updated: May 24th, 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