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 Policy: What it is and Why - The Basics

A security policy is nothing more than a well-written strategy on protecting and maintaining availability to your network and it's resources. By having a well-written policy that covers the following areas, you should be able to react and recover from most situations in minimal time: 1) Risk Assessments 2) Password Policies 3) Administrative Responsibilities 4) User Responsibilities 5) E-mail Policies 6) Internet Policies 7) Disaster Recovery and 8) Intrusion Detection. But regardless of whether you are on a Local Area...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Security Policy
What it is and Why - The Basics
Joel S. Bowden
February 18, 2003

Introduction:

To start off I would like to insert a quote from the GIAC Basic Security Policy Ver. 1.4 February 27, 2001. I have been trying to put into words what a good security policy is and what it does. After reading the above-mentioned material I couldn't find a better definition.

> *"A security policy establishes what must be done to protect information stored on computers. A well-written policy contains sufficient definition of "what" to do so that the "how" can be identified and measured or evaluated.*
>
> *An effective security policy also protects people. Anyone who makes decisions or takes action in a situation where information is a risk incurs personal risk as well. A security policy allows people to take necessary actions without fear of reprisal. Security policy compels the safeguarding of information, while it eliminates, or at least reduces, personal liability for employees."*

A security policy is nothing more than a well-written strategy on protecting and maintaining availability to your network and it's resources. By having a well-written policy that covers areas listed below, you should be able to react and recover from most situations in minimal time.

- Risk Assessments
- Password Policies
- Administrative Responsibilities
- User Responsibilities
- E-mail Policies
- Internet Policies
- Disaster Recovery (Backup and Restore)
- Intrusion Detection

But regardless of whether you are on a Local Area Network (LAN) connected or not connected to the Internet, or the CIO responsible for a large Wide Area Network (WAN), a security policy is a must.

So, with the following information I hope to give you a basic overview of what a Security Policy is and why you would want one. From here lets move on to some of the areas mentioned above

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

and why they are so important to you, your business, customers, administrators, and users. Basically everyone involved.

Risk Assessment:

Risk Assessment is something that should be done prior to putting your design into action. The assessment will give you a roadmap to securing your network infrastructure. By performing an assessment you can answer several questions that will improve the security of your network. These include what needs to be protected, what risk do these assets face, and what or how much of an upgrade will it take and what you will need to add to meet your business needs. In other words how much is this going to cost. So hopefully you had your budget in mind while developing your plan.

When performing the assessment keep in mind that risks don't just come from Hackers and Crackers. Don't forget about Mother Nature who can reek havoc on a network, disgruntled employees and those employees who mean no harm, but just haven't received the training needed. So the categories basically look something like this:

Mother Nature	Those Who Mean Harm	Do not mean Harm Never the less Dangerous	Hardware
Fires / Floods	Hackers	UN-trained Employees	Power Failure
Hurricanes	Crackers	Contractors unfamiliar with security policies	Product Failure
Earthquakes	Disgruntled Employees		

Needless to say the Risk assessment is a very important step in your network security in that it gets you started in identifying your many assets and what it will take to meet your goal.

Now that the assessment is complete and you are headed in the right direction it would be a good idea to have a meeting with all those that will be effected by this security policy. This doesn't mean every single user or possible contractor. But the heads of each department, such as Help Desk, Research and Development, Finance, CEO. I think you get the point. The reason for this is, these are the people who will be using and supervising the people whom will be accessing the information on the network. They will be able to provide you with valuable information that will help in the rollout of the policy. Each department will have there own little nuances, which must be addressed. When you have your meeting lay out the categories you will cover that needs their input and then start with each topic and explain to them why this is needed and these are the options. People are more willing to change when they understand the why and how and have a little ownership in the process. Now lets move on and go over a few of the categories.

Password Policies:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

This is a very important aspect of the security policy. This can be any company's weakest link. It is vitally important that all users of your network understand the importance of keeping their password secret. In one area that I went to work in users were writing their passwords on the desk calendars, sticking them under their keyboards, and actually using post-its to stick them to there monitors. Why! Because there was no set policy in place governing passwords and if there were any, none of them were aware of it. Needless to say what could have happened if an unauthorized user had come in and accessed the network. The only way we could have made the hacker's job easier was to just give them the password. If a password needs to be written down ensure this is included in the policy on how this will be handled. It could be that they are placed in a sealed envelope and placed in a safe with an access list. It all depends on your situation. So ensure that you cover the administrators responsibilities and the users responsibilities in respect to passwords. As for the password itself here are a few things not to do.

Passwords should **not** be any of the following:

- dictionary words (including foreign and technical dictionaries)
- anyone's or anything's name
- a place
- a proper noun
- a phone number
- passwords of the same character
- simple pattern of letters on keyboards
- any of the above reversed or concatenated
- any or the above with digits prepended or appended

http://www.mhpcc.edu/accounts/password_policy.html

Administrator Responsibilities:

The administrator has many areas of responsibilities therefore I will only touch on a few for the purpose of this paper. One area that is overlooked is that many operating systems, routers, hardware VPN solutions, and switches come with default accounts and passwords. These should be dealt with right out of the box. A good rule of thumb is to change the administrator accounts names and to disable any built-in account that won't be used. As far as the default user name and password accounts on the hardware, change them immediately. If a Hacker is out to be malicious and he as done a footprint on your network and has determined what hardware and Operating system you are using, you can bet he knows the default account names and passwords too. So do not make his work any easier for him.

Another area the administrator is responsible for and needs a good plan/policy is the assignment and maintenance of passwords for the users. This will vary depending on the needs of your company. Some will feel they need to know each users passwords and possibly assign the passwords themselves. Others will not want to know the user passwords but retain the permissions to change them in the instance they are compromised or the user forgets the password. This is another area that must be explicit in your policy. How the administrator can positively identify the user so he can change the password or unlock the account? This can be

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

especially difficult if you have remote users who can not come to you for authentication. So here is another aspect of your security policy that must be addressed.

User Responsibilities:

First for the user to be responsible, that person must know of and understand the security policies in place. This means a good training program should be in place to indoctrinate new and old employees when this policy is rolled out. Depending on the size of your operation there are many methods that could be used. Some companies use newsletters, others use CBTs or just email with the topic included. A few of the areas, which need to be covered, are the importance of password security, rules governing removable media (Diskettes, CD's, etc…), computer usage (personnel use, email, Internet). The key is to ensure your users are trained and up to date.

E-mail Policies:

Now here is a little subject that has caused many companies, businesses, the Military and other Government Agencies numerous heartaches, downtime, and money. If this doesn't convince you about E-mail policies let me name three other good reasons: "Melissa", "I LOVE YOU", "ANNAKOURNIKOVA" these are 3 well known email attachments that reeked havoc on email servers across the world. Here is an excerpt from the Cert. Summary CS-2000-022 on the "I Love You" virus.

> *"The "Love Letter" worm is a malicious VBScript program which spreads in a variety of ways. As of 5:00 PM EDT(GMT-4) on May 8, 2000, the CERT/CC Coordination Center had received reports from more than 650 individual sites indicating more than 500,000 individual systems were affected. In addition, we had several reports of sites suffering considerable network degradation as a result of mail, file, and web traffic generated by the "Love Letter" worm".*
> http://www.cert.org/summaries/CS-2000-02.html

Just imagine something like this happening on your email server. Do you have a plan in place to recover from such an event? At the time I was working at a Military location and they ended up shutting mail servers down until a way to clean up the systems was derived. Imagine the effect that had on the communication channels of that base. Imagine what it could do to your business. Just another good reason for a comprehensive, yet flexible security policy.

Still not convinced? Then look at it at this angle.

> *"Not convinced that it's necessary? Look at any recent court case. Opposing attorneys now ask for email the way they used to demand inter-office memos. Microsoft's prolonged anti-trust case is a prime example of the effect of company email on a trial.*

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Beyond legal ramifications, consider the negative publicity and damage to your company's reputation that could be caused by the wrong email getting out. "

You Have To Have An Email Policy
http://management.about.com/library/weekly/aa071299.htm

In your email policy you would want to cover personnel emails. You know the ones. Jokes that everyone forwards to each other yet could be offensive and create a very unhappy workplace. How about those slide shows that are sent around with all the pretty pictures and stories. If everyone were allowed to just send and forward this type of email you could just about create a self-inflicted Denial of Service.

Internet Policy:

The Internet, a wonderful compilation of information that's just a click away. Unfortunately there is a lot of information just a click away you can do without. So you would definitely need to develop a usage policy covering the use of the Internet. If you had your own web servers and firewalls then the policy could be as simple as filtering out certain URLs. Or it could be a detailed list of what a user can and cannot do on the web. It should discuss what type of sites is forbidden and if the Internet will be used for business purposes only or if there is any leeway for personnel use. No matter what you decide is right for your needs, just make sure the users are aware and understand.

Backup and Recovery (disaster recovery):
When you did your Risk Assessment hopefully you determined what information is critical and needs to be backed up and that which may not. No need spending money and time on something that is not of any importance or value. Backups are highly important for numerous reasons.

- System Crashes and you loose all data
- You are an unfortunate recipient of a virus
- The computer itself is stolen
- Hackers deface or destroy your data
- Users accidentally delete there files
- Natural disasters – Lighting, fires, floods, hurricanes

So has you can see backups are pretty important. Your policy should have and specify plans for:

- A backup schedule – when, how often, ideally you wouldn't schedule them during peak hours.
- What type of backup – Full, differential, incremental or a combination
- What type of equipment will be used – tape, CD, hardrive
- Where will the backups be stored – on site in a safe, off site, or a combination of both?

There is nothing like a good backup plan to help you through an UN-expected crisis. Remember the policy is there to protect your data.

Intrusion Detection:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

There is a lot of commercial intrusion detection products out there so when you start looking at how to secure your network. Do Your Homework. Make sure the product you chose is going to fit your business needs. In other words don‘t by a vault when a lock box would do the job. This portion of the policy should cover from, what type of Network Intrusion Detection (Network Intrusion detection is a device placed on your next work to monitor traffic coming and going). Host Base Intrusion Detection (Host Based is placed directly on the system to be monitored.) all the way to what is consider an event or incident and how is it reported within your company? It should cover in writing whether or not vulnerability scanning is allowed and if so who is responsible to perform these scans and when. If there is an incident how will it be handled. Will those on shift have the authority to attempt to thwart the break in? Or will they be required to contact a supervisor to get this permission. No matter what you decide is right for your business, make sure it is concise and it is precise in who is responsible for what action. And it spells out what authority each person involved has. You don't want someone standing around scratching his head because he isn't sure what he is authorized to do next or doesn't know whom to call.

Summary

With this subject I could go on for days but I won't. I just hope that by reading this you have a better understanding of what a Security Policy is and how important it can be. So in closing let me leave you with one last item because I feel this is of utmost importance to your policy.

If you do not have a good training avenue in place and your users are not aware of or do not understand the policy in place then it isn't worth the paper it is written on. So do yourself a favor. Train! Train! Train! In the long run you will only save your self time and money.

References:

SANS "GIAC Basic Security Policy"
Ver. 1.4 February 27, 2001, page 3 paragraph 2 and 3

Kerberos Password Policy For MHPCC
URL: http://www.mhpcc.edu/accounts/password_policy.html

Windows NT Domain Password Policy Recommendation
URL: http://www.aff.cornell.edu/as/it/password_policy.html

Agency Password Policy Model (As Submitted by the State Agency)
URL: http://www.oit.state.ar.us/Arch/Domains/Security/password.htm

A guide to managing remote users. By John Shireley
URL: http://www.networkcomputing.com/netdesign/1107remote.html

Intrusion Detection
URL: http://www.robertgraham.com/pubs/network-intrusion-detection.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

You Have To Have An Email Policy
URL: http://management.about.com/library/weekly/aa071299.htm

IEEE Email Policy
URL: http://eleccomm.ieee.org/email-policy.shtml

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 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**