GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

What makes a good security policy and why is one necessary?

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table of Contents

What makes a good security policy and why is one necessary? 1
Introduction 3
Why have a security policy? 3
What Makes a Good Security Policy? 4
What Is Included in a Security Policy 6
First Section – Parameters 6
Second Section – Risk Assessment 7
Third Section - The Actual Policies 8
Conclusion 11
References 12

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Introduction

With the advent of the Internet and networking, there has been a huge potential for expanding the way that businesses communicate and share data, provide services to clients and process information to increase their efficiency and lower production costs. It is now possible to interconnect two partner companies in order to share data in real time, hold conferences with people who are geographically separated and to place orders and update inventory in real-time. However, this broad access has also brought with it the possibility for data theft, liability through disclosure of private information, loss of credibility and reputation. The threat comes from people both internal and external to a company. There are many individuals with the potential to create havoc and disrupt businesses, maliciously or unintentionally, creating financial loss and impeding production. It is now possible for "hackers" to write code that will delete all the data on a system, steal sensitive or critical information and bring a company to its knees through denial of service attacks.

As these threats have increased, security has become a priority for companies. Securing systems from internal or external threats can protect companies from the potential liability arising from any type of network compromise. However, there are no quick fixes when it comes to network security. Security does not come from automated applications, rather it is compromised of security applications or systems, processes and procedures and the personnel to implement both the systems and processes. In order to properly address security, the most fundamental item necessary is a security policy.

The Merriam-Webster definition of a policy is "a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions" or " a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body". A security policy states the corporation's vision and commitment to security, and lays out its standards and guidelines regarding what is considered acceptable when working on or using company property and systems. A good security policy is compromised of many sections and addresses all applicable areas or functions within an organization.

Why have a security policy?

Having a security policy is instrumental in creating a secure organization. This is because without one, a company cannot begin to know where or what to purchase or what processes to follow in order to secure their environment. The policy lays

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

out, in detail, what the company's goal is for security. In other words, a security policy establishes standards for what is permitted or denied within the framework of the company. Standards are created for protecting the network resources and for assigning program management responsibilities and providing basic rules, guidelines, and definitions for everyone in the organization. Before you can implement a firewall, for example, you need to know a company's security policy on Internet usage and what is permissible.

Security policies help to create consistent standards across the organization. In this way, risks are avoided and penalties are outlined for failure to adhere to the regulations within the policy. A policy also identifies the roles and responsibilities of everyone within the company in ensuring security. Hopefully, a policy will be clear enough and inclusive enough to be easily implemented and followed. It is also important that the policy be flexible enough to encompass and accommodate a wide range of data and many different systems, activities, and resources.

A security policy is also another way of establishing the importance of security within the organization. A security policy is usually published and includes endorsement by upper management. In this manner upper management provides tacit acknowledgement of security as a company priority. This helps to establish the cooperation of an organization's personnel.

What Makes a Good Security Policy?

A good security policy is compromised of several factors. The most important factor is that it must be usable. A security policy is of no use to an organization or the individuals within an organization if they cannot implement the guidelines or regulations within the policy. It should be concise, clearly written and as detailed as possible in order to provide the information necessary to implement the regulation. It should be versioned and dated in order to easily identify the most current document, and should be structured internally in such a way that pertinent or required information is identified and located easily within the document for reference.

A good security policy also takes into account the existing or implicit rules in use. Business processes evolve over time within organizations as personnel learn more efficient ways of processing information. A security policy should in no way impede or interfere with the business. Rather, it should enhance the process, providing confidence in the security of the day – to – day operations.

It must be enforceable with security tools where appropriate, and with sanctions where actual prevention is not technically feasible. Firewalls, intrusion detection

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

systems, anti-virus applications are some of the tools that can be used to apply the policies in the business environment. However, manual processes should be laid out within the policy, as not every security policy is enforceable via an automated system or application. One of the most common misconceptions is that security policies are driven only by security systems. In actuality, it is the processes outlined within the security policy, and the people who carry out the required policies that create a secure environment.

Local, state and federal laws should also be considered when creating the security policy. There are many statutes and laws governing the privacy of certain records, dealings with outside parties and access violations. Those responsible for writing the policy should become familiar with the laws in their particular industry and location, and strive to have the security policy conform to them.

In a similar vein, a security policy should also specify what auditing processes will be put in place to verify compliance, and the punitive actions that may be taken in the even of non-compliance of any of the stipulated regulations.

The interests of employees, third companies and the business goals of the company should always be considered in a security policy. For instance, security policies that make provisions for the privacy of personnel information take into account the sensitivity and importance of safeguarding their employees. It is just as important to take into account safeguarding the assets of any partner companies.

When creating a security policy, it is a good approach to have drafts reviewed by representatives from different departments, such as IT managers, legal and human resources personnel and executives. This will create a document that is a representation and addresses the concerns of all interests within the organization.

Purchasing decisions can be influenced by security policies, as products will need to address security as outlined within the document. Therefore, a good security policy will help to create standards for software, hardware and other supporting network equipment.

Security policies will also help to clarify what actions should be taken, and the people to be notified, in specific situations. This aids in prompting users to take actions sooner and hopefully to prevent or lessen the impact of any security violations. The policy should also detail what corrective actions should be taken after the breach, and any legal or criminal penalties that may be pursued in certain situations.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Security policies that are well thought out and inclusive will always help in providing guidance and directives for policies in other areas. Privacy is an area that should be addressed not only by security but also, legal, human resources and management.

Finally, a security policy is a living document, and as such, in order to be effective should be reviewed and updated on a periodic and regulated basis to ensure that it is up to date and covers all applicable situations, environments and systems within the organization.

What Is Included in a Security Policy

A security policy contains many sections but these can usually be grouped into three categories. The first category outlines the parameters that are used within the policy. This section can have many subsections. The second area usually defines a risk assessment, or accreditation, process and the last area is the one with the rules and guidelines formed using the information from the second section.

First Section – Parameters

Introduction
The introduction at the beginning of the document usually explains why the security policy is being implemented at the site. Basically this is a summary of why the policy was created, whose authority was used to create the policy and what the policy addresses.

Audience
The second part of the parameters section addresses the intended audience, who the policy was written for, usually the general population of a company, including regular users, IT personnel, managers, etc. Along with whom it is intended for, the Audience section also addresses what part of the policy is applicable to each audience group.

Definitions
In order to ensure that everyone who reads the security policy comes away with the same understanding of the stated rules and regulations, including a definition of the terms used within the policy is essential. This avoids any misunderstandings, unintentional misrepresentations or lack of comprehension of policy because of lack of comprehension of terms used within the policy.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Second Section – Risk Assessment

Including a risk assessment of resources serves a few purposes. The most important and most obvious reason for a risk assessment is in order to quantify the risk associated with the systems. There is a cost associated with applying security to an organizations assets; money is spent on security tools, appliances and applications. What a risk assessment does is to make sure that money is not spent inappropriately, on systems that do not warrant the spenditure. An inventory of systems is usually performed in conjunction with a risk assessment. A risk assessment will determine what threats exist for systems within an organization and how high the risks are for those systems. The results will help to prioritize systems from those of highest threat to areas of minimal exposure and vulnerability. This will aid in identifying those areas where the highest level of security should be focused and how those areas should be protected. The goals of securing assets are to provide the maximum levels of availability, integrity and confidentiality, and a risk assessment should always judge threats and exposures with regard to how these three areas will be affected by them.

It is unusual to go in depth into the subject of risk assessment within a security policy. Rather, a security policy is used to state system categories and their security classifications. The categories are used to identify the systems within an organization and classification addresses the level of security needed to provide the optimum security protection. Threats to each category of system will usually dictate their security classifications. The classifications will be further defined by listing the threats that are faced. Finally, security measures will be determined based on classifications.

Identifying Assets

Assets are not limited merely to hardware, software and related equipment, such as valuable proprietary information and applications and sensitive data. Company assets will also include the personnel involved in daily business functions, documentation, processes and supplies that are used to support those business functions. The categories that are used within a security policy are usually subjective and determined based upon the priorities of business.

Threats to the Assets

Unauthorized or malicious access or theft or disclosure of sensitive data and denial of services are just a few of the threats faced by company assets. Many companies will have simulated attacks performed on their assets, either by qualified in-house personnel or third party security firms. These simulated attacks are designed to highlight and pinpoint the vulnerabilities within an organizations systems and architecture, including the human component. These simulations serve the added purpose of also identifying the greatest vulnerabilities and most exposed systems to those vulnerabilities. This

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

information can then be used to create the risk assessment guidelines discussed in the introduction to this section.

Third Section - The Actual Policies

There are many sections that come under this heading, but not all will be included in any given security policy. Only those sections, which are pertinent to an organization, are listed within their security policy. Some companies also make their security policies more specific than others. In a distributed and decentralized organization, policies should remain as non-specific as possible, and cover the broadest range of issues without being platform specific. Listed below are the broad headings that cover most of the important items to be incorporated in a security policy, along with general guidelines about what them.

Security Planning and Oversight

Security planning and oversight involves the establishment of a security department as a recognized entity within the business hierarchy. Under this heading the roles and responsibilities of the security department are defined. The responsibility of security planning and incorporation is usually assigned to members of the security department, working closely with the affected business groups. Oversight of security implementation, compliance and policies are also under the governance of the security department.

Security Education, Training and Awareness

It is imperative, if security is to be taken seriously, that an awareness of security be propagated throughout the organization. A security awareness program that incorporates security training and education is the best way to accomplish this goal. Security training raises awareness of the possibility of security breaches and the myriad ways in which breaches can be performed. Training educates users as to how to protect themselves, their environment and ultimately the business. It gives personnel the information necessary for them to prevent, detect and mitigate any violations. It also provides examples so that people can recognize threats when they witness them.

In a large and decentralized environment this training is particularly necessary because those business units not geographically close to the personnel of the security department need to be instructed in whom to contact and what items to include when reporting any suspicious incidents.

Backups and Business Continuity Plans

In the event of a breach, backups are vital in restoring daily operations. Policies should dictate the information to back up, the method used in creating backups, the archival policies and retention period for backups.
Catastrophic events include not only security breaches, but also natural disasters, environmental failure such as fire and bombs, and human tragedy where lives,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

property or the capability to perform vital business functions are threatened or seriously impacted. After such an occurrence, it is imperative that mission critical systems be brought up, at alternative locations if needed, and put into production in order to prevent the total failure of the business. Emergency response plans should be detailed to include backup operation plans, procedures and responsibilities.

Physical Security
Often overlooked, physical security is part of the security policy. This section should include physical access controls used to restrict or deny entry to sensitive areas. It should detail procedures for admitting visitors entry to business offices and the access provided to personnel employed at the business.

Facility requirements should be included here. Requirements include air regulation, fire safety equipment and measures, temperature and other environmental controls as required for normal business functions.

Access Controls
Access involves much more than simple entry to the facilities. Access permitted to documents, sensitive or otherwise, files and directories, proprietary information or systems are also a large part of access controls. The processes used to approve access to systems and information should be laid out here, including the procedures used in the event of employee termination. Do not forget to include remote access by employees, extranet connections for outside companies, and access to public areas.

Authentication
Authentication is the methodology used to determine that a user is who they state they are, and that they have the required credentials to access certain areas. The standard for authentication should be spelled out, whether it is simple password challenges, two-tiered authentication schemes or the more sophisticated biometrics in use today. Incorporate within the standards the policies governing them, including how many attempts at authentication are permitted before locking access, how robust the specific method used should be (for example, the length and characters used in a password determines how strong it is and the degree of difficulty in guessing it), inactivity logout periods, etc.

Network Security
Network security states how assets on the network will be protected. Assets include, but are not limited to, data whether proprietary or public access, servers, routers, and applications. Security controls used to secure these assets may include firewalls, intrusion detection systems, access controls, authentication methods, network auditing, operating systems used and file system directory structures.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Encryption
As encryption, or the process of converting clear and readable text into undecipherable algorithms in order to protect and ensure privacy, has evolved into a widespread technology. It is used over wide area networks, to create digital signatures verifying user authenticity, and to protect data that travels over the public domain, such as e-mail. In order to prevent a lack of usability and confusion over what type of encryption to use, a standard should be detailed and the configuration used listed.

Acceptable Use Policy
The acceptable use policy states how users are allowed to use company resources. This includes Internet, e-mail, server, data, equipment, and personal use limitations of all resources.

Auditing and Review
Once the policy has been disseminated and implemented, a procedure to check user and equipment compliance should be instituted. The auditing and review policies should lay out the frequency, time frame and methodology to be used in reviewing and auditing compliance. This is useful in identifying and correcting gaps in security before incidents occur. It is also helps to ensure that should a breach be identified the company will have legal or punitive recourse with which to address the involved parties.

Compliance
Compliance explains the enforcement policies for the security policies. It may include the penalties associated with non-compliance and the process used in investigating any suspected non-compliance. This helps by preventing the ignorance excuse that has been presented in the past in order to excuse security transgressions.

Incident Handling and Response
One of the most important areas within the security policy, the Incident Handling and Response section points out and educates personnel about identifying security breaches. The outcome of a security incident can sometimes hinge on the timely detection and notification of the incident, and what steps are taken to mitigate the breach. It can mean the difference between a minor incident and one where major losses, either in production or monetary, are incurred. In here are the processes to follow during specific incidents, including natural and other disasters. Who to notify, what to do, what information to provide, and extenuating circumstances should all be laid out here along with a prioritization of incidents.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Conclusion

Not everything that should be included in a security policy can be detailed in any one document. When creating a security policy, take into account the business function, the corporate culture, the budget and resources at your disposal. Be sure to include all pertinent personnel in the policy creation process in order to include all areas deemed of interest and priority. A good security policy is so much more than just a listing of regulations. It dictates the scope, direction and priority that security within an organization. A good security policy can mean the difference between a comprehensive security posture and a document that is neither regarded nor implemented with any conviction. Security begins with the policies that are enforced within an organization, and a large budget does not ensure success. What does ensure success is a good policy that is descriptive, disseminated and enforced within a company.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

1. http://csrc.nist.gov/isptg
2. http://www.sans.org/newlook/resources/policies/policies.htm
3. The Internet Security Guidebook: from planning to deployment by Juanita Ellis and Timothy Speed
4. http://downloads.securityfocus.com/library
5. http://www.ietf.org/rfc/rfc2196.txt?number=2196
6. http://secinf.net/info/policy/hk_polic.html
7. http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2196.html
8. http://www.sun.com/software/white-papers/wp-security-devsecpolicy

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.