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 benefits do Security Policies provide Network Administrators?

GSEC Security Track 1 Practical
By Tracy D Coyle
19 November, 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract

Planning to run a network under controlled conditions requires a sense of humor with a long standing admission that a system administrator's job would be proportionally easier without all the pesky users. The only sensible way to implement an element of security within the hedge of users and administrators is thru the use of security policy. The sense of humor comes into play when creating these rules to live by and admission that rules only keep honest people honest. This creates the need for a publication of immense depth regarding how the members of an organization can best use the resources available locally and through the Internet.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Introduction

In every instance of human history, man will push the limits of the personal, regional, social or cultural norms…despite any existing guidelines. So that leaves one item left; how to address user needs for network use and balance some construct of user policy. This may be a document, presentation, speech or merely a disclaimer that shows up in a logon script. These are meant to inform, to educate, to regulate and theoretically protect all parties from impropriety. At the user level is where any policy written or published must be geared. Differing rules of access may apply to executives and others in leadership positions with widespread interests within the network infrastructure from general employees with access granted simply towards their specific role.

The varying choice of access levels that may apply within your infrastructure are hard to express to your non-technical co-workers as is, how to control the users holding that access. The potential of software or features to the systems that ride the pertinent network demand a learning curve beyond none and leave you with much planning to do. Verbage must be non-technical in nature in order to prevent misinterpretation. If this does not exist, an unwary user claiming stupidity or worse may wreak havoc when problems arise. What instances would be of concern to the existence of a secure network that may be compromised by not heeding or providing current and correct policy? Although policy may cover specifically a single issue, corroborating evidence may allow an otherwise obvious infraction from going unreported or ignored.

Policy in place

Perhaps your policy addresses the point of not forwarding any official business emails to commercial servers. This prevention has supposedly been addressed through use of Outlook Web Access and Microsoft Internet Information Server for all non-local communications. This seems easy enough to use but a multiple of factors can cause a displaced employee or one industrious worker planning for an away trip to arrange resources be made available readily through the use of commercial email. Therefore aiding access to pertinent information regardless of location.

Policy for the technologically inclined

The ease with which businesses embrace telecommuting folds a new element of protection for administration hoping to keep their jobs. There are numerous avenues for threats, whether perceived or realistic, to threaten the livelihood of those responsible for providing computer users the ability to conduct their network-based affairs and not risk additional compromise through excessive and unnecessary policy when the simplest of approaches may work best.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audits and their place in policy

A common practice in both recently adopted and well-established networks is it either have an internally-monitored review, or the preferred manner in which an independent company is asked to test the integrity of a network. The reasons for an audit can be multifaceted, but one can certainly validate the level in which users comply with existing policy. The documentation following a comprehensive analysis of a network through auditing holds an element of demonstratable evidence that problems exist. Policy and its impact on the conduct of an audit are meant neither to be a "fire and forget" weapon, nor a panacea of all things risky to data. Controlled tests can easily show where users are either blatantly or unknowingly in violation of agreements for network use, whether written or implied. Even the most junior network administrator would be quick to react to some issues that are brought to light in review of an audit. The "knee-jerk reaction" to fix it as you go through the policy review and audit is self-defeating. It has been demonstrated numerous times recently that sweeping and more effective changes can be employed when the cumulative issues brought up by a completed audit are addressed in their entirety.

Events that should be contained in logged results of audits **(REF 1 p 62)** can include but are definitely no limited to:

- Logins (successful and failed)
- Logouts
- Failed access to files or system objects
- Remote Access (successful or failed)
- Privileged Actions (such as those taken by administrators, both successful and failed)
- System Events (such as shutdowns and reboots)

Each event should as well capture and log the following information:

- User ID
- Date and time
- Process ID
- Action performed
- Success or failure of the event

There should as well be written guidance governing who is responsible for parsing audit logs, what format and media type the logs are to be kept, the manner and schedule in which they are accessed, and how long of time period they should be kept in archive status. Use of programs such as **Log Parser (REF 2)** from Microsoft Corp. can be used to ease the parsing and use of audit logs through the conversion to a command line utilization.

Patching and updates

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Policy has been addressed for end users in many forms and variations of terminology. This does not, however, prevent the effective use of written guidance governing administrators and those responsible for placement, segmentation, documentation and bulk administration of networks in all levels of service. There is no need to over-exaggerate the need for current versions of all pertinent programs such as web servers, file sharing, proxies, remote access and various patches that apply to service provisions. Some may certainly be outsourced to vendors in charge of providing updates on service contracts. Other administrative programs should be held locally responsible, both for accountability and credibility in training. Amplification to existing policy can include references to regularly scheduled service times. As well, long-standing agreement with vendors may be evaluated for a push program allowing updates to be generated on an "as generated" basis.

Policy creation considerations

Generation of a comprehensive security policy for a sample network regardless of size or purpose must be considered though all of the three following regards. There is no hard and fast rule for using only the precepts from these three thoughts, and nothing preventing them from being combined for a particular goal.**(REF 1 p 59)**

The first type of policy consideration is the purpose. Each policy, regardless of the audience, should plainly express why these guidelines are being established or enforced, and what the organization desires the result of compliance will be. There can be no room for interpretation when the purpose is stated. Doing this will greatly increase the acceptance and employment of said policy.

The next type of expression a policy is to consider is the scope in which it is meant to operate. The target group the policy is suitable for must address general ands specific network access needs and/or separation by billet or intent.

The last of the requisite types of policy considerations is the need to define the responsibility of each and every compliant user. This empowers all persons granted access to network resources a level of the organizational authority. Plainly this can prevent issues from arising before damage or infractions are made. This decentralization of network responsibility for conduct allows users to "police their own". The atmosphere of a shared regard will have a contagious affect on all users. This awareness that either simple mistakes or the blatant threat to a network's integrity by denying the policy in place, affect not merely an individual host. More importantly, it can illustrate how rapidly widespread damage can affect an organizations use of resources. Company wide loss or decline of communications via phone, email, web-based services, incorrect assessments of company requirements through milestone calendars, and the all too often publicized loss of sales through wholesale or retail venues.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In recent times, responsibility delegation has been viewed as the correct way forward, bringing many benefits: **(Ref 3)**

- Availability of the information pertinent to the security need can be accessed in a timely manner relevant to requirement.
- Decentralizes information concerning security from one point of information to many and reduces administrative costs and personnel across a wide spread network.
- Assignment of responsibility for security requirements. This also them seem that they are taken more seriously and will not be overlooked or ignored blatantly.
- More visible and demonstrable compliance with legal, regulatory and organizational requirements. These can be local municipal or federal references and must be stressed at all levels of access.

Access controls

Controls of access to data networks must be held in the forefront of all things regarding policy creation. Some form of user-defined access controls must be available for each resource on the system.

Policy standard of affect

There has to be a compulsion from the policy writer's perspective to tell the users what they can and cannot do. This must encompass their own job as well and focus on the preparation of the network for day-to-day operations in as safe of an environment as possible without making the job impossible to do. This can include, but is certainly not limited to the following: **(Ref 5)**

- Regularly install new Microsoft security patches – Necessary patches for Microsoft program vulnerabilities often come out on a weekly basis. If available for use in your network, the Windows Update needs to be run regularly to ensure the latest round of worms, virus and other vulnerabilities have been patched. This may prevent unknowing vulnerabilities from becoming certain risks.
- Use of anti-virus software – Use of this software, either server-based or host-based, is a given in today's networks.. Because of it's prevalence in today's market, Windows is more popular for attacks than any other operating system and viruses are generally specific to holes inside the code written for Windows applications. Virus definitions must be updated

© SANS Institute 2003, Author retains full rights.

regularly and must be supervised to be applied appropriately. One example is a batch file run at user login to allow the server-based definition file to traverse the network from a shared drive to the user machine and import to the user-based software for update. If not, the presence of this software is completely without merit. New viruses and worms come out constantly so keeping the latest virus definition on your machine will reduce the risk of infection. Attention must be paid to the source of the data input from where the viruses may come and what manner it is read through the hardware. This may include the use of modems and network cards of many different types. Each may possess a unique set of vulnerabilities.

- Install spyware blocking software - There are many freeware and shareware anti-spyware applications that will help mitigate the threat of spyware, software that was unknowingly installed on your computer and is used to watch you or track your movements on the Internet.

- Install spam blocking software – This has become one of the more popular items to plan for in governing use of policy and how to keep the efficiency of your network at its peak. Use of these can relieve the stress of babysitting users who regularly receive emails from commercial vendors or may accidentally place themselves on mailing lists and receive unwanted traffic. This can regularly slow if not cripple a mail servers performance. Spam often contains pesky viruses or scams, so if you can find a spam blocker you like, compare the properties of several and use your most suitable choice.

- Change password(s) - Make them strong, and change them often. Also, make sure not to use the same passwords used on external networks, such as Amazon.com in case those sites are compromised without your knowing. For more information on good password practices, see: "The Simplest Security: A Guide to Better Password Practices." Also, if you run Windows XP, beware of hidden accounts and passwords. Check to make sure every account is secure, and create a schedule for changing passwords regularly. It's a pain, but it's important.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Disable ActiveX and Java in Internet Explorer - Both of these technologies are regularly exploited in malicious web pages and can be used to infect your computer with viruses, worms, trojans, or spyware. Unfortunately, disabling ActiveX in recent versions of Internet Explorer causes a warning to be displayed when visiting legitimate sites that use this technology.

- Disable auto-download or auto-open features - It's difficult to know what comes in and out when programs have free reign to transmit at will, particularly with applications that you've installed and forgotten about. Disabling those that auto-transmit lowers the chances of attack.

- Turn off file and printer sharing - If you don't need it on your network, disable it. This should be a given, as file and printer sharing should never be made available over the Internet by a home user but may certainly find use in corporate enterprise, where resources are more limited.

- Consider a new method of receiving email - It's a sensitive topic, but email programs are historically full of security holes, particularly in the areas of attachments and HTML rendering. To be sure yours isn't one of those, do a little research. Install the latest version of whatever program you choose, and configure it such that attachments are not automatically downloaded or executed. This is more useful than any virus checker. Keep in mind that the more popular a mail program is, the more it will become a target. Outlook Express is a prime example of this. Keep on top of the security patches offered by the vendor, as many attacks are based on holes that were discovered (and patched) many months before.

- Utilize a hardware/software firewall – Devices such as routers may provide some level of filtering for protection but are not a catch-all. Popular hardware platforms may be inexpensively employed throughout your network and as well the use of common software-based filtering such as ZoneAlarm may be used. It's an elementary step taken to protect new PCs that may be added to your home or enterprise network.

- Compare and contrast use of various operating systems - Windows is a very popular platform for exploits. If this is the sole operating system for you, during your next computer purchase consider augmenting or changing completely to an alternate operating system. MacOS X still has

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

no confirmed viruses spreading in the wild, compared to more than 65,000 viruses for Windows-based computers. Or try Linux or other generally free to use open-source operating systems on your desktop.

- Backup – This is a commonly overlooked process that should be kept very much in the forefront of every operators mind when analyzing processes. Keep full backups as well as incremental backups. With the price relative to storage media growing more affordable every day, there is no excuse for not having a well-planned solution. Offline or offsite storage in case of natural disaster or other emergency is as well a fine reason to plan for other areas of backup media locations.

© SANS Institute 2003, Author retains full rights.

Conclusion

With the wide variety of goals in today's network administration, it would seem almost unthinkable that such variances would exist in the development and use of security policy. For such a network intensive environment as organizations have become lately, there may be some credibility to the acronym of KISS (Keep It Simple, Stupid). No longer do administrators have to start from scratch in determining the nature of security policy. Now with the available resources of decades of making the attempts, and occasionally publicizing the mistakes made in creation of user policies allows all to learn and not delay deployment of such documentation. One can be bold and discuss the ever-present risk **(REF 7)** that administrators face when referring to their networks as ready for the users to "Login".

© SANS Institute 2003, Author retains full rights.

References

(1) Joel Shore, “Inside a Security Audit”
Network World, October 20, 2003.
URL: http://www.nwfusion.com/research/2003/1020audit.html

(2) Microsoft Corp Log Parser 2.0 Aug 2003.
URL:
http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=8cde4028-e247-45be-bab9-ac851fc166a4 (Nov 10, 2003)

(3) Seymour Bosworth and Michel E. Kabay; “Computer Security Handbook 4”
Wiley (New York), ISBN 0-4717-1258-9
URL:
http://www.amazon.com/exec/obidos/ASIN/0471412589/tag%3Dfusion0e/103-6976773-0079000 (Nov 10, 2003)

(4) The Security Policies & Standards Group
Portland House
Farringdon Lane
London EC1R3AU

URL:
http://www.information-security-policies-and-standards.com/compliance.htm

(5) Sarah Granger, ”Home User Security: Your First Defense”
SecurityFocus.com - collection of articles
URL:
http://www.securityfocus.com/infocus/1746

(6) Eric Manwald, “Network Security: A Beginners Guide”
Osbourne/McGraw Hill (New York), ISBN 0-07-213324-4
(2001)

(7) Joel Weise and Charles R Martin, “Developing a Security Policy”
Sun Blueprints Online – December 2001
URL: http://www.sun.com/solutions/blueprints/1201/secpolicy.pdf

© SANS Institute 2003, Author retains full rights.