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: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

SECURITY AWARENESS – EVERYONE'S BUSINESS

Security awareness is the fundamental basis for all your security processes. Security awareness is

"The process by which you make everyone on your network aware of what your security policies and practices are, what is expected of them, and how they handle your information."[1]

If your users are not aware of what the policies and procedures are, then it becomes very difficult to maintain the security with regards to user ids, passwords, and file access. Security awareness training makes security everyone's business. No policy or procedure is effective unless it implemented in such a manner that the end users play an important role in building on that foundation. Without cooperation on all levels, most security practices could inadvertently be breached, leaving a potential problem in maintaining the integrity of your data or resources.

Introduction

After many years as an end user in the business, I transferred into a security administration role within my company. Needless to say, I had to be made aware of what "security" was. This included logical security as well as physical security. The company is now moving towards a knowledge-based business with an open-office attitude. My role has now changed into a more pro-active stance, assisting the users to understand what files "everyone" can read and which ones should still have more stringent security. My task now is to balance security, with more availability, without compromising the integrity of the data.

Laptop Security

Laptops are very convenient to use but pose their own unique security risks. Cable locks for laptops are now readily available for most laptops on the market today, and should be used, no matter where the laptop is stored.[2] When travelling, these can be a deterrent when used in hotel rooms or car trunks. More sophisticated locking systems are available with audible alarms for those laptops that contain highly sensitive information. Various tracking mechanisms are now available as well and should be used particularly when travelling.[3] BIOS (Boot) passwords can be used to protect the laptop data if an unauthorized person should attempt to log on. The system will not load if the password is incorrect.[4] Files on the computer can be encrypted, and have password protection to safeguard their integrity. Backups of the laptops should be done on a regular basis to ensure the data is recoverable if the machine is stolen.[5]

Physical Security

A fundamental part of security awareness is the physical aspect, which is often overlooked or ignored. In additional to the basics as listed above for laptops, you must protect other sensitive equipment and data. All servers should be in a

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

secured area that is monitored and reviewed regularly. Admissions to these areas should be available only to those who have shown a clear business need to enter those areas. The area can be monitored by audio/visual hardware. Access can be restricted by the use of a proximity or card swipe reader, and the issuing of those cards can be reviewed on a regular basis. Automatic door closures ensure the area is not left open accidentally.[6]

Any hard copies of files with confidential data should be locked up when not in use. Data classification should play an important role in determining when and if those files should be secured. Coding of files for internal use could help remind users which files are never to be left open and unattended. All files should be stamped with their classification. Data owners must be responsible for classification of their own data, since only they can determine the value of this asset. A classification document, listing the criteria for each classification, should be readily available to everyone.

A random physical review should become part of a regular audit procedure. This will reinforce the physical aspect to some degree. By doing a simple walk around after hours, you can obtain an overall picture as to how well the users are following policy and standards. You can check to make sure laptops are secured and computers logged off. Files should not be left out where anyone can read them, and file cabinets should be locked. A brief note to the manager of each department could let them know if they are advancing in this aspect, or where their weaknesses might be. For those who have abided by the policy, perhaps a short thank you note would be in order, helping to maintain their pride in that accomplishment. By reinforcing the idea of security on a regular basis, it becomes more of a habit instead of an inconvenience.

Logical Security

Logical security is, of course, a little more difficult to maintain. It also covers several aspects and can be broken down into many categories. I will briefly describe some of those aspects that are crucial to maintaining that portion of security.

Access Requests:

There should be a standard procedure in place for all access requests, no matter what the request. All requests should come from a manager or if for a manager, the next level of authority. No user should make access requests for him/herself since there has to be an accountability factor. There should be a clear audit trail to follow in order to validate any access a user may have. Access should be reviewed on a regular basis to make sure it is not carried from position to position.

Passwords:

Having a password policy does not mean that users will abide by it. Often people do not realize that if they give their password to another user, that person is now impersonating them on the network. Perhaps asking the user a few brief

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

questions will reinforce the policy on multiple usage of the same id. Questions could include:

Would you let that person cash your pay cheque and represent you at the bank? Would you let them take a driver test for you? Get a passport with your name? Then why would you let them be you on the network?

By using daily examples, users may understand the reasoning behind having individual ids and passwords, and the necessity of protecting those.

Having a strong password will prevent second-guessing a password by others. Teaching people to pick secure passwords can be simplified by using a process such as picking a passphrase and then using the first characters of each word. It will not work for everyone but it will at least encourage some people to tighten up the password portion somwhat.[7] Other common specifications for strong passwords are simple things such as not using names and dates for passwords. There are many factors to be considered when choosing a password. The password policy for the company should incorporate as many of these items as possible.[8] A list of criteria can be found on many Internet sites, including universities home pages, such as University of Texas at El Paso [9] and Edith Cowan University .[10] Many of these give concise instructions on how to choose a strong password that can be adapted to fit any business. Other factors to be accounted for are expiration dates, length of password, lockouts after a specific number of attempts, and duration of the lockout. These need to be defined in your policy as well.

File/Directory Access:

File access is another aspect of logical security. By setting up a directory with a clear standard for content, users will know what their limitations are for directory and file access. A public area could be set up for information that is not sensitive, can be used company wide, and has no real impact on the business if compromised. Other areas can be secured as required for normal business needs. Data classification plays an important role in this area as well, since that is what will dictate the security requirements. All data must have ownership assigned to someone who can determine the value of it, as well as authorize access requests to that data. Documentation on various applications and procedures for requesting access should be made widely available for everyone.

Standards and Policies

As I was researching security awareness, the most often preached process was having a security policy. Without a security policy in place, it is very difficult to implement even basic security measures. The security policy and standards currently in effect should be in an area readily accessible by all users. If is easy to find, people are more likely to use it as an information source. The policy must include standards for as many aspects of security that you fit your company's needs. Outlines for basic policy and standards are available on several sites, as are some off the shelf products. [11] The SANS Institute reading room has one paper, written by William Farnsworth, that covers quite an extensive list of items that need to be considered. [12] When I visited sites for universities, the policy was found easily on the

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

home page of these sites. Clearly it is a very important factor in promoting security awareness.

The policy must state in clear and concise terms what is deemed as acceptable usage of your network and resources. It should outline the various aspects that are addressed in the policy, including a password policy, privacy policy, email usage policy just to name a few. Because information technology and business requirements are ever changing, the policy and standards must be reviewed on a regular basis. What applies today may be a mute point in the future. Therefore a scheduled semi –annual or annual review would keep your policy and standards in line with the current business needs. It would address issues that otherwise might be overlooked with new implementations of software, hardware or business practices.

Although I have only touched briefly on this subject, there is more precise information available on many sites that will assist in designing and implementing a security policy. I will include some resources available to everyone at the end of this document. Please visit the sites for more information.

Enforcing the Policy:

Once you have implemented your security policy, you must be able to enforce it. Otherwise the policy is merely another document. Auditing can play a major role in this factor. An audit procedure must be in place to validate usage of resources on your network. The policy must include the ability to audit any of the key items cited in the policy, including such things as password compliance and business usage of email or resources.[13] You will need to develop a auditing process for checking compliance with any of the provisions stated in your policy. [14] Management plays a key role in this area since you will need their acceptance of this procedure in order to audit successfully without recrimination. The auditing process must include procedures to follow when unacceptable usage is detected or suspicious activity is noticed. There are many resources available to assist in developing an audit procedure, [15]as well as several tools that can be used.[16] Your audit policy can be developed in conjunction with the standards policy to make sure you cover the necessary items.

Auditing should be turned on for those objects that it is prudent to review. Logon and logoff, file or object accesses are a few of those that should be deemed as necessary. An auditing log, outlining which objects were audited and when, must be maintained in order to monitor activity on the network. A separate one for each server/process/or application could be created or they could be incorporated into one that could be manipulated to show pertinent data for each individual process if necessary. This log should also contain any comments or notes pertaining to the activity noticed at the time. For restricted resources or susceptible areas, the activity or event log should be reviewed on a daily basis. It is much easier to notice unusual traffic on your network if you already know what is normal. If users are aware that their activity may be reviewed at any given time, some might be deterred from "non-business" usage. Knowing that there may well be consequences to their actions will also act as a deterrent. Developing an audit process to fit the company's needs may be a time consuming task, but it will prove to be a valuable asset once implemented.

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

Security Awareness Training

Once you have implemented your policy, your most difficult task now begins; that of educating the user community. Training the users on security awareness can be done without a large financial output. Time to conduct the training is likely to create the most impact on a security department. Since managers are usually the biggest drawback, perhaps training for them could be implemented in short information sessions that would not interfere too much with their busy schedules. It is easier to bring the employees around to secure thinking if their managers are abiding by the rules.[17] Determine how management would best benefit from these sessions, and then work on pointers taken from the policy currently in place. Brief handouts for them to give to their employees might help.

The training process for security must fit the company image so it will have to be personal to your company. It would we well worth the time to meet with Human Resources department members to develop an awareness training schedule. Orientation for new employees should include a short section on security policy and procedures. It could include such things as demonstrating how to pick a strong password, what procedures for requesting access are, and basic physical security procedures. An employee handbook could be used to incorporate not only the employee benefits and provisions, but also security guidelines.

Tips of the day or week are another good idea that could be used without putting any stress on the day to day production environment. Brief emails outlining guidelines to follow could be issued on a monthly basis. Quick reference guides could be handed out at training sessions, as well as such items as stress balls, mouse pads and pens. Posters could be displayed on prominent bulletin boards. The company could create screen savers with tips or guidelines that could be installed by each user. Several could be created that reference key points in the policy.[18] Most people will view security as a drawback, until you validate the security process and back up the reasoning with good solid evidence. An informed user is less likely to place your data or equipment at risk. If the basis rules are outlined and simplified, users are more likely to practice them, on an ongoing basis, especially if taught from the beginning of employment.

Reporting of security violations does not come easy to most people. If a process is put in place to make reporting simple and anonymous, if necessary, more people might be encouraged to take action. A mailbox could be created just for that purpose with a response going back to the sender indicating that the information received would be treated in the strictest confidence. A secure voicemail system could also be utilized in that manner. By creating an atmosphere of trust on the confidentiality of the information received, people are more likely to be forthcoming with that information.

Conclusion

Security and security awareness cover a broad spectrum of ideas and processes. Risk and risk assessments are other aspects that I have not touched on, but need to be incorporated in the overall development of your policies and

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

procedures. There are a number of newsletters, digests and magazines that are available that cover a wide range of topics, some of which are cited here. There is a wealth of information and ideas on the Internet that you can customize to fit your business needs and user community.

Training people to think securely is not an easy task. It is an ongoing process, with no end in sight. With cooperation from the end users though, it is not such a daunting task. It then becomes a matter of reinforcing the idea of "mind your own business" in a much broader aspect. "Information security is everyone's business."[19]

For further information on specific topics:

Sun, Ann. " Securing Your Internet Connection".06/17/1998.
http://www.webpak.net/~misuc98/nsaf1/index.htm

Kelly, Jessica. "Computer Security Information" 08/21/2000
http://www.alw.nih.gov/Security/security.html

Computer Security Products Inc
http://www.computersecurity.com

CBOSS "Tips: Avoid Your Own Computer Nightmare"
http://www.cboss.on.ca/tips.html

University of Minnesota, Office of Information Technology
http://www1.umn.edu/datasec/security/security.html

Georgia Institute of Technology. "Computer and Network Usage Policy"
http://www.oit.gatech.edu/security/policy/usage/contents.html

Security-Audit.com
http://www.security-audit.com

Rybczynski, William. "Information Systems Security User Awareness: Social Engineering and Malware" 11/18/2000
http://www.sans.org/infosecFAQ/securitybasics/awareness.htm

Johnston, Kevin. "Online Information Security Assistance" 08/31/2000
http://www.sans.org/infosecFAQ/start/sec_assistance.htm

Ehinger, David P. "Considerations for an Acceptable Use Policy for a Commercial Enterprise" 11/22/2000 http://www.sans.org/infosecFAQ/policy/considerations.htm

Troffer, Lawrence. "Information System Security: How Much is Enough?" 08/21/2000
http://www.sans.org/infosecFAQ/policy/iss.htm

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

Hill, Michael. "An Overview of Computer Security Issues for the new Computer User" 12/20/2000 http://www.sans.org/infosecFAQ/start/issues.htm

Norton, Stephen. "Circle of Security" 11/13/2000
http://www.sans.org/infosecFAQ/securitybasics/circle.htm

Boston, Terry. "The Insider Threat" 10/24/2000
http://www.sans.org/infosecFAQ/securitybasics/insider_threat2.htm

Grove, Phillip A. "Electronic Data Security Awareness" 11/29/2000
http://www.sans.org/infosecFAQ/securitybasics/electronic_datasec.htm

Hernandez, Ernest D. "Network Security Policy – A Manager's Perspective" 11/22/2000
http://www.sans.org/infosecFAQ/policy/netsec_policy.htm

Hering, Jim. "Network Security on a Shoestring" 12/15/2000
http://www.sans.org/infosecFAQ/securitybasics/shoestring.htm

Set Solutions, Inc
http://www.setsolutions.com/security.htm

Pentasafe Security Technologies, Inc.
http://www.baselinesoft.com

Gamma Secure Systems Limited
http://www.gammassl.co.uk/index.html

For further information on various related topics:

Fred Cohen & Associates. "Strategic Security Intelligence" 05/05/1999
http://www.all.net/CID/Defense/Defense36.html 03/2001

An Introduction to Computer Security: The NIST Handbook
http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
http://csrc.nist.gov/publications/nistpubs/800-14

Information Security
http://www.infosecuritymag.com

Computer Security Institute
http://www.gocsi.com

SANS Institute
http://www.sans.org

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

Information Systems Security Association
http://www.issa-intl.org

CorpNet Security, Inc
http://www.corpnetsecurity.com

Security News.org "Security News for Security Professionals"
http://www.securitynews.org/index2.html

Telafortis Systems, Inc
http://www.telafortis.com/publications/RFC2196.htm

Telafortis Systems, Inc
http://www.telafortis.com/publications/RFC2504.htm

References

[1] Northcutt, Stephen. "Information Security: The Big Picture

[2] Thaddeus, Jude. "Laptop Security Turns on 65-Cent Solution" 10/18/2000
http://www.securityfocus.com/headlines/8908

[3] Childers, Robert. "Laptop Computer Security" 10/30/2000
http://www.sans.org/infosecFAQ/homeoffice/laptop.htm

[4] Purcell, Jim. "Securing Information on Laptop Computers" 12/27/2000
http://www.sans.org/infosecFAQ/travel/sec_info.htm

[5] McIntosh, Janet E. "Laptop Theft" 12/27/2000
http://www.sans.org/infosecFAQ/homeoffice/laptop_theft.htm

[6] Ashcroft, Dave. "Physical Security: The Often Overlooked Weakness" 07/31/2000
http://www.sans.org/infosecFAQ/firewall/phys_sec.htm

[7] Curry, David A. "Improving the Security of Your Unix System"
http://irm.cit/nih.gov/security/pwd_guidelines.html

[8] Donovan, Craig. "Strong Passwords" 06/02/2000
http://www.sans.org/infosecFAQ/policy/password.htm

[9] University of Texas at El Paso, University Security Committee. "Information Security Awareness"
http://www.utep.edu/infosec

[10] Edith Cowan University, IT Division Information Security
http://cowan.edu.au/ITDivision/security/aware.htm

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

[11] The Information Security Policies/Computer Security Policies Directory
http://www.information-security-policies-and-standards.com

[12] Farnsworth, William. "What do I Put in a Security Policy? 08/10/2000
http://www.sans.org/infosecFAQ/policy/policy.htm

[13] Berryman, Fred. "Employee Right to Privacy: Perceived or Real? 10/22/2000
http://www.sans.org/infosecFAQ/legal/employee_privacy.htm

[14] Naidu, Krishni. "How to Check Compliance with your Security Policy" 01/30/2001
http://www.sans.org/infosecFAQ/policy/compliance.htm

[15] Kapp, Justin. "How to Conduct a Security Audit" 07/2000
http://www.itp-journals.com/nasample/t04123.pdf

[16] Computer Audit, Systems Audit and Information Security Audit Made Easy
http://www.securitypolicy.co.uk/securityaudit

[17] Nichol, Kelly. "Implementing a Security Awareness Training Program in Your Environment for Every Day Computer Users" 12/18/2000
http://www.sans.org/infosecFAQ/start/awareness.htm

[18] Hisey, Patty. "Computer Security Awareness Training...Do you need it?" 12/20/2000
http://www.sans.org/infosecFAQ/securitybasics/training.htm

[19] Miller, Jon."Information Systems Security:Lessons Learned" 09/04/2000
http://www.sans.org/infosecFAQ/securitybasics/lessons_learned.htm

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