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 Awareness Training and Privacy

An organization's security policy sets the standard for the way in which critical business information and systems will be protected from both internal and external threats. Security policy must adapt to changing needs within the organization. Personnel responsible for creating and maintaining the security policy must learn to recognize changes in technology that impact security and how those changes impact the organization and the people who work for the organization. A key concern in today's society is the privacy of...

Copyright SANS Institute
Author Retains Full Rights

AD

CounterTack
Counter Tack Active Monitors
for In-Progress Attacks
GET THE
WHITE PAPER
NOW >>>

Security Awareness Training and Privacy
Michelle_Johnston_GSEC_v1.2e

Introduction

An organization's security policy sets the standard for the way in which critical business information and systems will be protected from both internal and external threats.

> Defining a security policy is an opportunity for an organization to simultaneously define and refine its collective attitude to both its internal operations and external relationships, and, as such, embraces all aspects of the organization's operations, not just those directly impinged by "IT". (Lightfoot)

Security policy must adapt to changing needs within the organization. Personnel responsible for creating and maintaining the security policy must learn to recognize changes in technology that impact security and how those changes impact the organization and the people who work for the organization.

A key concern in today's society is the privacy of individuals. The advances in technology have made it possible to store vast amounts of information about people at very little expense. Technology has also made it possible to access that information in a matter of seconds. Confidential information about a person can be accessed by parties unknown to the individual.

Security awareness programs are designed to educate users on the security policy of an organization. The goals for a security awareness program should include not only education about the organization's security policy but should help to foster an understanding of how the policy protects the business, the employee, and customers. One important thing to consider is whether or not it is good practice to inform employees what type of email and Internet access logs are kept by the organization. Security awareness training should educate employees at a high level how monitoring tools are used and what information can be gathered by those tools.

Security Awareness Training – Security Policy

Security awareness training in most organizations focuses on familiarizing the employees with the organizational security policy. The security awareness focus for users may include:

- educating users on the creation of good passwords
- do's and don'ts for maintaining workstations
- informing users of email and Internet access policies
- employee responsibility for computer security

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

- reporting procedures
- emergency procedures

The focus for security awareness for system administrators may include:

- training on how to configure systems securely
- education on user account management policies
- secure remote access for support of systems

Security awareness must also reach the business or non-technical user. Security awareness training for business users may emphasize:

- how to identify social engineering tactics
- how establishing and enforcing security policies can impact the "bottom line" (limiting system downtime, protecting business critical information, etc.)
- public relations impact of DoS attacks, viruses, etc., and how security standards can help limit this risk
- increase in productivity generated by using standard, locked down systems to minimize user downtime

In addition to the items listed above, information on tools used for monitoring Internet access and email should be provided as part of the security awareness training program.

Training system administrators, IT and business management in security is crucial. Management and system administrators need to realize that most critical security threats come from the inside. Logging user activity, monitoring email and Internet access are important pieces in being able to track internal security breaches.

According to a survey conducted by **eWeek** and Camelot IT, Ltd., 57 percent of the respondents said that attacks from outside were a more serious threat than those from inside. This is in spite of the fact that 57 percent of those responding who reported a breach in security, reported the breach was caused by insiders with unauthorized access. Forty-three percent reported that security was breached using accounts left open after employees left the company. Of the total respondents, 21 percent reported attacks from disgruntled employees. (Lightfoot)

If information technology professionals and CIO's believe that most threats originate from the outside in spite of statistics indicating the opposite, business managers will also share this belief. This point of view impacts the way in which security policy is interpreted by business managers. It also impacts the extent to which business managers will support and encourage adherence to security policy.

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

Business security is based on four main principals:

- protecting information
- maximizing operational effectiveness
- minimizing corporate liability
- protecting the corporate image

Communicating these principals to business managers and emphasizing how a security policy is designed to maintain these principals will ensure acceptance and support of the policy.

Security awareness training programs should strive to tie together policy, the effective use of monitoring tools for enforcing policy and the benefits to the business of a successful security policy.

Employee View of Security

Security awareness training can assist in tempering the attitude that security policy is restrictive and interferes with an employee's ability to do his or her job. It can also make management aware of the potential internal security threats. The more education people receive about security, the more they understand the importance of security and the ways in which security protects them and actually enables them to do their job in a more effective environment.

A security policy that is rigid and complicated to comprehend will be difficult to communicate. Policies that are flexible and allow management to decide what action should be taken when abusive behavior has been noticed are the most effective. These policies can allow decisions to be made based on current circumstances, priorities and available resources. (Wood) Policies can take a moderate position instead of a hard line allowing room for various levels of action to be taken when there is a violation.

The use of tools for logging and monitoring of Internet or email activity should be primarily for the enforcement of policy and the protection of the organization. Both management and employees must be informed on how these tools are used so they understand the correlation. Education about these tools can also be seen as a way of protecting the employee and not as an invasion of privacy or as a way to gather "evidence" for dismissal. Knowledge of what information can be gathered in logs can actually be a deterrent for misuse of company systems. (Schulman)

Monitoring Tools

Many new monitoring, filtering and reporting tools are now available and are relatively inexpensive to implement. A study by the Privacy Foundation found

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

sales of monitoring and filtering software had increased by sixty to eighty percent in the past two years. (Schulman)

Programs such as Websense, WebSweeper and SurfControl provide monitoring and filtering of Internet activity. Filtering is done by creating policies blocking access to certain types of sites. The policies can be based on groups or departments and can be turned on or off at specified times to regulate Internet use during the business day. Reports can be generated by these programs that summarize:

- number of connections made by a user
- browse time
- sites visited
- categories of sites visited
- attempts to visit blocked sites

Programs that monitor email such as MIMESweeper and InterScan eManager provide virus protection and content security. Email content scanning products check inbound and outbound messages for confidential data, excessive file size, and prohibited content. These programs search for keywords, spam, profanities and malicious code as well as banned file types. As in the Internet control products, policies can be set by individuals, departments or groups.

Examples of reports that can be generated from these tools can be used as part of security awareness training so employees are aware of the type of information that can be gathered about their web activity. Use of these tools should be related to the security policy so that employees understand what is being monitored or filtered and why.

Monitoring Tools and Policy

Policy on the use of the Internet varies from organization to organization. Some companies may see Internet use as distracting and a problem that must be controlled. Other companies may see the Internet as a creative resource to further its business. Whatever the policy, monitoring policies should directly support the enforcement of that policy and not go beyond the boundaries needed to enforce policy.

For example, the following Internet use policy would be enforced by monitoring Internet traffic and email.

> Associates are encouraged to use the Internet in the course of conducting daily business, keeping in mind that this exploration should be appropriate for their job responsibilities and workload at the time. All usage should be appropriate to Company's environment, values and best interests.

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

The company in this example would not use any type of content filtering. Monitoring could be done by using firewall or proxy logs or a program that was designed to analyze those logs. This type of monitoring would be sufficient for support of this policy.

The policy below could be enforced by a content filtering program:

> Email may not be used for knowingly transmitting, retrieving, or storing any communications which are: (a) of a discriminatory or harassing nature, (b) derogatory to any individual or group, (c) obscene, offensive, indecent, sexually explicit or otherwise pornographic, or (d) of a defamatory or threatening nature.
> Forwarding of Company information or internal memos outside of the company using Company email, Internet email or any other electronic media source is not allowed unless it is an authorized function of your job duties.

In both of these examples, showing employees the type of reports that can be generated from logs or demonstrating the action that will be taken by content filtering programs should be part of the security awareness training program.

Privacy Concerns

Notice of monitoring, whether in the employee handbook or a banner warning displayed at login is not adequate notification of ongoing continuous monitoring of online activities. In a time where debate is ongoing about the legality of keeping information on individuals in databanks, organizations need to ensure that employees are clearly informed of the policy and the method of monitoring.

By logging and storing a detailed audit trail of employee activities, organizations may inadvertently create potential evidence. This evidence could be used against them by a disgruntled employee claiming that they were not informed of the type of information being collected about their Internet activities.

Telling employees what monitoring system is in place and explaining the system's capabilities are likely to be more of a deterrent than a vague reference to "your activities may be monitored for enforcement purposes."

Conclusions

In the rapidly changing world of technology, security policies must be created that fit the current environment and are flexible enough to adapt to change without becoming obsolete. Establishing security policy that fits the environment of the organization helps create a link between adhering to the policy and the success of the organization. Security awareness training can help strengthen this link by

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

educating management about internal security threats and how effective monitoring tools can assist in reducing this threat.

At the same time, employee privacy must be protected. It is no longer possible to rely on "notice" about Internet and email monitoring practices. Security awareness training is an excellent forum for informing employees about monitoring tools that are used by the organization and what type of information is logged and stored. Educating employees about monitoring programs and how they are used protects both the employee and the organization.

Resources

"InfoSec in the Real World: A Pragmatic Approach to Implementing a Corporate Security Policy", Derek Lightfoot, http://securityportal.com/articles/infosec_realworld20010716.html

"Insiders are main computer security threat", Dennis Fisher, EWeek, June 20, 2001. http://www.zdnet.com/eweek/stories/general/0,11011,2777325,00.html

"The Extent of Systematic Monitoring of Employee Email and Internet Use", Andrew Shulman, Workplace Surveillance Project, July 9, 2001. http://www.privacyfoundation.org/workplace/technology/extent.asp

"Business Issues Relating to Content Security and Policy Management", white paper, Chris Heslop, April, 1999. http://www.mimesweeper.com/products/collateral/pdfs/whitepapers/content_security.pdf

Wood, Charles Cresson. "Blocking, filtering and censoring Internet traffic", Computer Security ALERT, April 2001, p. 9-10.

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

Quiz Questions

1. True or False. Security policy should be flexible to meet the changing needs of the organization and advances in technology.

2. Business security is based on four main principals. Which of these listed below is NOT one of those principals:

   a. improving corporate image
   b. protecting information
   c. minimizing corporate liability
   d. maximizing operational effectiveness

3. Security awareness training should include which of the following:

   a. what type of password hacking tools are available
   b. how to gain access to confidential information in an emergency
   c. what type of tools are used to monitor Internet and email activity
   d. details on the internal network infrastructure of the organization

4. True or False. A banner displayed at login is sufficient notice to employees of ongoing continuous monitoring of online activies.

5. Tools used for monitoring Internet or email activity should be used primarily for:

   a. Gathering evidence to fire employees
   b. Enforcement of security policy
   c. Determine which Internet sites are most often visited by employees
   d. Censor outgoing email

6. Content filtering programs use which of the following to regulate Internet activity:

   a. firewalls
   b. filters
   c. policies
   d. passwords

7. True or False. According to surveys, most information technology professionals believe more serious security threats come from the outside.

8. Email content scanning programs search for all but which one of the following:

   a. Keywords

© SANS Institute 2001, Author retains full rights

b. Malicious code
c. Banned file types
d. Incorrect email addresses

9. True or False. The privacy of individuals is becoming more of a concern in today's society.

10. True or False. Security awareness training programs should emphasize the consequences of violating security policy.

© SANS Institute 2001, Author retains full rights

Last Updated: May 19th, 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**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**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**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**