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

SANS GSEC Practical

The Importance of Security Awareness Training

Beth Jensen
GSEC Practical Version 1.4b
March 10, 2003

© SANS Institute 2003, Author retains full rights.

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

The Importance of Security Awareness Training

Abstract

We all know that auditing, monitoring, applying security fixes, patches, staying on top of technology and having a security policy are all excellent measures in keeping a company's infrastructure secure. However, one important element that sometimes gets overlooked is security awareness training.

Ecommerce has dramatically changed the way we do business. Just over the past five years we have gone from shopping at the mall or via catalogue to shopping from home over the internet. Because of this, it is time to focus on educating the users on the risks and vulnerabilities. One way to address this task is through security awareness training.

There are two aspects to delivering a successful security awareness training program. The first is determining what should be included in the training. The second is the aspect of determining the delivery method for the training. This paper will cover some of the details of each of these aspects.

Definition

What is security awareness training? The National Institute of Standards and Technology defines security awareness training as:

> Awareness, training and education controls include (1) awareness programs which set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure, (2) training which teaches people the skills that will enable them to perform their jobs more effectively, and (3) education which is targeted for IT security professionals and focuses more on developing the ability and vision to perform complex, multidisciplinary activities[11].

Now I will cover some of the main areas of focus within security.

Sensitive Data

A crucial element is to define sensitive data. What is sensitive data? Sensitive data is all data that is classified as confidential, data that should not be shared outside the organization, or trade secrets that would be of interest to another competitor. With additional laws forthcoming, personal information is also falling into this space.

Addressing the Weakest Link

People are a critical factor in ensuring the security of computers and the valuable data which they process. It is a well known fact that people are the weakest link in the

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

security chain[4]. It is management's responsibility to ensure that all employees are familiar with the company's security policies and procedures. Therefore, once users have been given access to data, they need to be aware that it is their responsibility to protect that data. This awareness can be communicated through a security awareness training program.

Password Management

Strong passwords are the first defense in stopping a hacker. Emphasis needs to be placed on the following password guidelines:

- Passwords should be changed regularly
- Require minimum password length
- Passwords should not be a word from any dictionary, in any language
- Passwords should not include personal information
- Passwords should never be written down
- Passwords should contain a combination of uppercase letters, lowercase letters, numbers and special characters
- Passwords should NEVER be given to anyone

Recently I attended a briefing that included a refresher course on security awareness. I thought it was interesting to hear how quickly a password could be cracked if the password was based on the criteria listed below:

Criteria	Length of time to be cracked
Word of any length in a dictionary	< 30 seconds
5 random letters	1 minute 15 seconds
4 random letters/1 number	2 minutes 55 seconds
7 random letters/1 number	4 to 6 days
6 random letters/1 number/1 special character	4 to 6 days
5 character lower and upper case with a number	approximately 15 minutes

Several of the password guidelines mentioned above can be enforced through software. For example, the minimum length of passwords, how often a password should be changed and using a combination of characters can be enforced with a Windows 2000 Domain Policy. There are also third party software tools available that can be used to enforce password complexity, such as "Password Bouncer" by Avatier (http://www.ig.com.au/PasswordBouncer.htm).

Passwords should be easy for the user to remember, but difficult for someone else to guess. One suggestion for creating strong passwords is to choose a favorite line in a song or phrase, take the first character of each word and convert some of the

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

characters to numbers and special characters and capitalize at least one character. For example:

"Take me out to the ball game" becomes Tm0ttbg!

This method would enable a user to create a strong password that would be difficult for someone else to guess.

Workstation Security

Users need to understand the importance of workstation security. Workstation security education should, at the minimum, include these key points:

- Stress the importance of locking the workstation with a password enabled screen saver
- Enforce the same password policy for screen savers as is used for sign-on passwords
- Remind users to lock their workstations every time they leave their desk
- Never give their screen saver password to anyone

Users need to be aware of the consequences if they don't follow the workstation security policy. If workstation security policies are not followed, an unauthorized person could gain access to:

- Data stored on the hard drive of a workstation
- Data stored on the network
- User's email
- Other employees hard drives
- Other platforms attached to the network
- Data that they might not have privileges for

Laptop Security

If an organization has issued laptops to their employees, then we cannot forget to educate the users on laptop security. Laptop theft is steadily on the rise, and is not just about the loss of hardware. These thieves are stealing the data they find on the laptops. The data on the laptop is likely to be worth far more than the hardware itself. The cost of stolen data is costing organization's billions of dollars. To avoid this, laptop users should:

- Physically secure the laptop at the desk by using a cable lock on the laptop and attaching it to the docking station or locking it in a desk drawer.
- Never leave the laptop unattended while traveling. Physically secure the laptop by attaching a security cable to the laptop and something heavy and stationary, such as a table or cabinet.

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

- Never leave the laptop in plain sight in the car. If you need to leave the laptop in the car, always put it in the trunk if possible. An additional defense would be to install and activate a motion detector or alarm when the laptop is left in the trunk.
- Never check the laptop as luggage, but take it as a carry on. Keeping the laptop with you will ensure that no one has tampered with your data.
- Never take the laptop through a metal detector. The hard drive could be damaged if sent through a metal detector.
- Don't send your laptop through airport screening detector until you are ready to step through yourself. Sending the laptop ahead of you could give someone an easy opportunity to run off with the laptop. Be sure to keep an eye on your bag until you claim it.
- Regularly backup the data on your hard drive, in the event that something happens to your laptop. The best recommendation would be to have users store data on the network. This will ensure that the data gets backed up on a regular basis and not have to rely on the user remembering to do regular backups.
- Never store confidential data on the laptop. If confidential data must be stored on the laptop, be sure that the data is encrypted.

Personal Digital Assistant (PDA)

Another portable computing device that is widely used today is the personal digital assistant (PDA). These devices are easily lost or stolen. Because of this, security has become a focus for these devices. Listed below are several ways these devices can be made more secure:

- Enable the power-on password feature
- Set the auto turn-off feature for idle time for 3 minutes or less
- The PDA should be synchronized regularly with the PC
- Install a data encryption software to encrypt the data stored on the PDA
- Install a virus detection and elimination program

All PDAs should be guarded carefully and kept out of sight. "Unfortunately, the only way to really secure a PDA is to lock it into a vault"[7].

Viruses

Viruses are an increasing threat to all computing systems. Due to the damage done by Code Red and Nimda, virus attacks are now being reported in the media. Because of this, users are more aware of virus threats. We need to remind users to scan all diskettes with virus protection software and never open suspicious email attachments. Originally, viruses were spread through infected .exe files. Today, they are spread mostly through Outlook via attachments. For company issued workstations, current virus definitions need to be updated by the IT Department on a regular basis. However,

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

end users need to be aware of keeping their virus definitions up-to-date on their home PCs.

Social Engineering

One topic that many users need to be more familiar with is social engineering. "The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network"[4]. Social engineers are able to get the information or access to systems that were intended for specific users. There are several techniques to effectively social engineer an organization:

- Impersonation is a one successful method of social engineering. Social engineers impersonating a system administrator or a management person tend to be very successful in obtaining someone's password. Help Desks are usually targets for impersonation. Users need to be attentive at all times and never give out their password to anyone regardless of the situation.
- Dumpster diving is another method of social engineering. This is where someone can gain personal and financial information by going through a company's dumpster. Employee and customer information, printouts of sensitive data, and interoffice memos are just a few items that dumpster divers are looking for. Any data that could pose a threat to the organization should be shredded. All confidential documents should be marked as such and kept under lock and key.
- Shoulder surfing is a popular method of social engineering. This is accomplished by looking over someone's shoulder as they type in their password or trying to see the information that someone is working on. Shoulder surfing can be eliminated by being conscious of the people around you and who may be looking over your shoulder while you type your password, enter your ATM PIN number or when giving out your credit card number.
- Sensitive information or data can easily be obtained just by eavesdropping. People need to be aware of anyone who might be listening during conversations that could be overheard. Don't discuss confidential or sensitive information on cordless phones or in public places. These discussions should take place with the appropriate people in a conference room with the door closed.

During my research on social engineering, every article I read mentioned the infamous Kevin Mitnick. Kevin Mitnick was able to hack into phone company networks through social engineering. However, he denies that he ever asked anyone for their passwords. He was able to get access to sensitive information by getting people to trust him. His ability to successfully social engineer cost him five years behind bars. I was told that Kevin Mitnick has written a book, "The Art of Deception: Controlling the Human

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

Element of Security", which details his social engineering skills. Unfortunately, I personally haven't had the opportunity to read his book.

Identity Theft

You can't discuss security awareness without mentioning identity theft. With identity theft on the rise in the United States, I think it would be beneficial to make users aware of this reality and how easily it could happen to them.

What is identity theft? Identity theft is when someone steals pieces of information about an individual and uses it to represent his or herself for fraudulent purposes. The pieces of information that someone steals could be:

- Social security number
- Mother's maiden name
- Driver's license number
- Address and telephone number
- Financial information, such as bank statements and credit card slips
- Employee badge

How do they get this information? Sometimes it can be as easy as:

- Stolen purse or wallet
- Stolen credit cards
- Access to bank statements and credit bills by stealing someone's mail.
- Dumpster diving

A Joint Publication of the Privacy Rights Clearinghouse and The California Public Interest Research Group (CALPIRG) has an excellent website that provides a list of resources that need to be contacted when someone becomes a victim of identify theft (http://www.privacyrights.org/fs/fs17a.htm).

Depending on the access assigned to an employee badge, a stolen badge is like having the "keys to the kingdom". For example, let's say the employee was a network analyst that had access to the secured Data Centers where both test and production servers existed. If his/her badge gets stolen, the thief now has access to all the servers in the Data Center. Stolen proprietary information and confidential data would be very damaging to an organization. Security awareness training would be a good time to remind employees that's it critical to report their lost or stolen badge to security immediately so it can be deactivated.

Wireless LAN

A more recent vulnerability that needs to be mentioned is the Wireless LAN. Wireless LANs are quickly becoming the latest technology to get installed in offices and homes. This technology appeals to the user because it allows them to be connected to the

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

network as they move throughout their home or office without being constrained by a cable. Instead of communicating with the network through a cable, communications are done through access points. The access point broadcasts a radio frequency signal announcing that it exists and is ready to provide service. The information that is broadcasted by these devices contains all the information necessary to join the network to which the access point is connected. This information is being broadcasted in plain text.

Due to the small cost, usually less than $200.00 for both the wireless card and router, along with ease of installation, anyone can setup a wireless network. Most individuals are setting them up within their homes. Because of lack of education, many users don't enable any security or encryption for their access point, or if security is enabled, it is the manufacturers default security. Many access point default configurations do not activate Wired Equivalent Privacy (WEP), or if it is enabled it is using a vendors default key.

This lack of security allows anyone with the proper equipment and knowledge to gain access to the network, and all devices on the network, through the access point. If one of the devices connecting to the access point is a corporate laptop, all the information contained on that laptop, unless it is properly secured by passwords and/or encryption, is open to the public. A great example of how an individual's home access point can provide a way into a corporate network is illustrated in the following article in Computer World's Daily Shark Tank archives.

> President of this big energy company lives a few miles from the company's downtown headquarters and wants to be able to work from home, reports a sysadmin pilot fish.
>
> "He has our telecom team put in a T1 line from his house directly into the corporate network," says fish. "So he is set up with a company-standard desktop and his very own file server back at the office and full, open access to the network -- just like being at the office."
>
> Which is fine at first. But then the president decides he wants to be able to access his e-mail using a laptop anywhere in his house.
>
> "So he goes down to the local computer retailer and buys a wireless access point," fish says. "He installs it himself and leaves everything at the defaults."
>
> Which means there's no encryption or security of any kind enabled on a wireless access point that's smack in the middle of a major city -- practically an invitation to war-driving hackers.
>
> Fortunately, the company's telecom manager soon hears about the boss's new wireless home network. "He had his team 'help' the president to set up his

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

wireless correctly, and replaced the $50 hardware with some hardware more suited to protect a global corporate network," says fish.

But that doesn't save the president completely from embarrassment. A few months later, an outside team of security auditors presents the results of its six-month audit of the company.

"They held a meeting with all the bigwigs of the company," fish says. "And what's at the very top of their list of security holes? You guessed it -- the president's home wireless network. They came across it when it was still a wide-open hole into the corporate backbone." [11]

Wireless Access Points are also being installed within companies without the knowledge of the IT department. Due to the relatively small cost and the ease of installation, many users have decided to bypass the hard-wired network using one of these wireless access points. Wireless Access Points installed within a business without the knowledge of the IT department can cause an even bigger security threat to the business than ones installed within homes. Once again this is due to the fact that they are not configured with the appropriate security and basically leave the door to the network wide open to anyone who wishes to enter.

A point that many people forget to consider is the range of the signal's transmission. Unless the access point is configured to limit the range of the signal, the range is limited only by signal degradation over distance, similar to a radio station. Currently, the average range of an access point is 300 feet, but Intel is working on a solution that would provide a signal that would travel 30 miles. Similar to a radio station, the signal can pass thru solid objects, like walls and floors. So if your company occupies one of four suites on one floor of a 50 story building, the individuals above you, below you, around you, and even across the street can receive the signal from the access point, and thus gain access to your network, unless properly secured.

Another point to consider is that there are more people sitting in the parking lot of a business trying to find an open way inside, than there are people trying to get into a persons home network. With an unsecured access point that can broadcast up to 300 feet or more, you are just sending an open invitation to someone to walk right into your network.

These are just a few of the many reasons that a security awareness program must include information pertaining to the hazards of wireless networks. For more information pertaining to the security concerns involved in wireless networking please refer to "Seven Security Problems of 802.11 Wireless"[15].

Security Policy

Another topic to mention would be the security policy. Users should be aware of the organization's security policy and how it's enforced. A security awareness training

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

program is of no value if you don't have a security policy in place to back it up. "One of the advantages of policies is that they remove the responsibility of employees to make judgment calls regarding a hacker's request. If the requested action is prohibited by policy, the employee has no choice but to deny the hacker's request"[5]. The policy should also include the organization's policy on using email and the Internet. If an organization has a monitoring policy, it is a good idea to remind the users that email and Internet usage may be monitored periodically to reduce the risk of improper usage.

Physical Security

Last, but not least, users need to be aware of physical security. I believe the events of September 11, 2001 have increased everyone's awareness for the need for increased physical security. Physical security not only protects information resources but also protects the employees. Employees should be aware how each point of entry has been secured. Examples of ways to secure points of entry may include:

- Doors that require badge security for entering and exiting
- Posting security guards at each entry
- Surveillance cameras at each entry to see who's coming and going

The employee should also be aware of anyone trying to tailgate into the building. Any suspicious activity needs to be reported to management.

Previously, I mentioned that the second aspect of security awareness training is determining the delivery method for the training. There are several different delivery methods that can be used:

New Employee Orientation

New employee orientation is a great place to provide security awareness training. This would also be a good opportunity to introduce new employees to the organization's security policy. After the presentation, each employee should be given an information security awareness pamphlet. This pamphlet should contain the security policy, a brief overview of the presentation, and an email address or phone number in case they have questions at a later time.

Videos

Another delivery method for the training is via video. Videos can reach large groups of people at the same time. These videos can be shown at unit meetings, department meetings or conferences. A video-based training program would provide the same level of training to all local and remote users. Videos would also be an excellent training method for the delivery of ongoing security awareness. They also provide a means of getting a consistent message throughout an organization no matter how large or small.

Posters

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

Posters can be used to address specific security issues, such as suggestions for strong password management. The social engineering or general security awareness posters should be eye-catching and present a single message. These posters should be strategically placed throughout the organization and viewed at eye-level. Materials should be designed to get people's attention. As a bonus you could include a tri-fold handout at these locations as an additional means of information. These handouts would have the poster on the cover and additional information inside.

Novelties

Novelty items can be used as constant security awareness reminder. These items can be imprinted with a variety of security information and distributed after new employee orientation or after security awareness training sessions. Examples of novelty items could include:

- Pens
- Notepads
- Magnets
- Cups or mugs
- Mouse pad
- Sticky notes

Self-Study Course

A self-study course would be a successful method of training as it allows employees the opportunity to complete the training as their schedule allows. However, you may need to make this course mandatory to ensure that all users complete the training. This method could also be used to deliver ongoing training.

Regardless of the method of delivery for security training, you need to keep it simple and fun. Using real-life examples tend to bring the point home better than just using statistics. People tend to remember circumstances surrounding real stories and real people. The goal of the training should be to get employees thinking about security all the time.

One final topic to mention during the security awareness training is the contact information for incident reporting. Users must know who to contact, how to contact that person, what information needs to be reported and when it should be reported. Below are a few suggestions for what type of information should be provided:

- Telephone, pager numbers or email address for incident reporting
- Give examples of types of information needed when reporting the incident:
    - Type of system
    - Location of system
    - Date and time of incident

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

    - Description of what is happening
- Inform the users when to report an incident via email or telephone
- Inform the users to report an incident as soon as it's discovered. Immediate reporting can prevent further damage.

Conclusion

In order to achieve overall success with a security awareness program, you will need to keep training materials up-to-date, keep users informed of latest threats and attacks, and provide ongoing training. Employees should be required to complete this training annually. Ongoing security awareness training helps to lower the risk of cybersabotage.

In today's world, security is the responsibility of everyone. Following the 9/11 attacks, President Bush reminded the American people that we need to be aware by keeping our eyes and ears open and report any unusual activity to the authorities. The same can be said for information security. Through security awareness training, we can make users aware of their responsibility to keep things more secure and encourage them to report any unusual activities. Security awareness training can provide a good line of defense.

© SANS Institute 2003, Author retains full rights.

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

REFERENCES

[1]Rudolph, K. CISSP, Numkin, Louis, and Warshawsky, Gale. Computer Security Handbook, 4th Edition, Chapter 29 (Draft), 2001. http://nativeintelligence.com/awareness/chap29-1.asp

[2]Verton, Dan. "Security Experts: Users Are The Weakest Link". Computerworld. November 26, 2001. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,66047,00.html

[3]Dedo, Douglas. "White Paper – Security on the Pocket PC". May, 2002. URL: http://www.microsoft.com/mobile/enterprise/papers/security.asp

[4]Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics". December 18, 2001. URL: http://www.securityfocus.com/infocus/1527

[5]Granger, Sarah. "Social Engineering Fundamentals, Part II: Combat Strategies". January 9, 2002. URL: http://www.securityfocus.com/infocus/1533

[6]Verton, Dan. "Companies Aim to Build Security Awareness". Computerworld. November 27, 2000. URL: http://www.computerworld.com/careertopics/careers/training/story/0,10801,54375,00.html

[7]Crouch, Cameron. "Tech tips: Keep your PDA data safe". PCWorld.Com. February 12, 2001. URL: http://www.cnn.com/2001/TECH/ptech/02/12/PDA.security.idg/

[8]VIGILANTe. "Social Engineering". URL: http://www.vigilante.com/inetsecurity/socialengineering.htm

[9]Janowski, Davis D, and Chang, Stephanie. "The Lay of the Wireless LAN". PC Magazine. May 21, 2002. URL: http://www.pcmag.com/print_article/0,3048,a=26038,00.asp

[10]Identity Theft: What to Do if It Happens to You
A Joint Publication of the Privacy Rights Clearinghouse and CALPIRG
http://www.privacyrights.org/fs/fs17a.htm

[11]Shark Tank: "Why security people get gray". Computerworld. February 28, 2003. URL: (http://www.computerworld.com/departments/opinions/sharktank/0,4885,78918,00.html)

[12]Andress, Mandy. Surviving Security: How to Integrate People, Process, and Technology. Sams, 2001: 436-439.

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

[13]Desman, Mark B. Building an Information Security Awareness Program. CRC Press, LLC, 2001.

[14]Schneier, Bruce. Secrets & Lies, Digital Security in a Networked World. New York, John Wiley & Sons, Inc., 2000.

[15]Gast, Matthew. "Seven Security Problems of 802.11 Wireless". O'Reilly Network. May 24, 2002. URL: http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html

[16]Avatier. Password Bouncer. URL: http://www.ig.com.au/PasswordBouncer.htm

© SANS Institute 2003, Author retains full rights.

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