Global Information Assurance Certification Paper

Social Engineering: Policies and Education a Must

Rick Tims

February 16, 2001

Introduction:

Social Engineering is the acquisition of sensitive information or inappropriate access privileges by an outsider, based upon the building of inappropriate trust relationships with insiders. It is the art of manipulating people into actions they would not normally take. The goal of a Social Engineer is to trick someone into providing valuable information or access to that information. It preys on qualities of human nature, such as the desire to be helpful, the tendency to trust people and the fear of getting in trouble. The sign of a truly successful Social Engineer is they receive the information without raising any suspicion as to what they are doing.

People are usually the weakest link in the security chain, and Social Engineering is still the most effective method of circumventing obstacles. A skilled Social Engineer will often try to exploit this weakness before spending time and effort on other methods to crack passwords. Why try to hack through someone's security system when you can get a user to open the door for you? Social Engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone. A successful defense depends on having good policies in place and educating employees to follow the policies.

Common Types of Social Engineering:

Social Engineering can be broken into two types: human based and computer based. Human-based Social Engineering refers to person-to-person interaction to retrieve the desired information. Computer-based Social Engineering refers to having computer software that attempts to retrieve the desired information.

Human-based:

- Impersonation – Case studies indicate that help desks are the most frequent targets of Social Engineering attempts. A Social Engineer calls the help desk pretending to be an employee. They claim to have forgotten their password and ask the help desk to reset it or give it to them. The help desk will frequently do this without verifying the identity of the caller. The Social Engineer will often know names of employees in the organization he is trying to penetrate, and he will have learned as much as possible about the person he is trying to impersonate.

- Important User - A common ploy is to not only pretend to be an employee, but to be a Vice President or other important employee in order to add an element of intimidation. A help desk employee is less likely to turn down the

request of a Vice President who says he has 10 minutes to get some important information he needs for a meeting. The Social Engineer may threaten to report the employee to their supervisor if they do not provide the information required.

- Third-party Authorization – The Social Engineer may have obtained the name of someone in the organization who has the authority to grant access to information. They may call the help desk or other personnel saying that "Mr. Big Shot" said it was OK to give him the information. This can be particularly effective if the person is on vacation or out of town. If the Social Engineer knows this information, he may say something like, "Before he went on vacation, Mr. Big Shot said I should call you to get this information."

- Tech Support – The Social Engineer may pretend to be from the technical support department of the organization or one of the organization's hardware vendors to gain information. They may call an employee and ask if they are having any computer problems. Since this is often the case, the employee may say they are. The Social Engineer then tells them he will work on their problem, but he will need their signon and password.

- In Person – The Social Engineer may enter the building and pretend to be an employee, guest or service personnel. They may be dressed in suits or uniforms, and will often be allowed to roam the halls unchallenged. They can look for passwords stuck on terminals, find important data lying on desks or overhear confidential conversations. Social Engineers often hire members of the organization's janitorial staff to look for sensitive information.

- Dumpster Diving – This refers to looking through an organization's trash for valuable information.

- Shoulder Surfing – Looking over someone's shoulder to try to see what they are typing as they enter their password.

Computer-based.

- Popup Windows – A window will appear on the screen telling the user that he has lost his network connection and needs to reenter their user name and password. A program previously installed by the intruder will then email the information back to a remote site.

- Mail Attachments – Programs can be hidden in email attachments that can spread viruses or cause damage to computer networks. This includes, viruses, worms and trojan horses, The attachments are often given names that entice the employee to click on them, such as "Fun Love" or "I Love You." The latest example is the "Anna Kournikova" virus. It makes the user think they will be seeing a picture of Anna Kournikova. It also is an example

of how Social Engineers try to hide the file extension by giving the attachment a long file name. In this case, the attachment is named AnnaKournikova.jpg.vbs. If the name is truncated it will look like a jpg file and the user will not notice the .vbs extension.

- Spam, Chain Letters and Hoaxes – These all rely on Social Engineering to be spread. While they do not usually cause any physical damage or loss of information, they do cause a great deal of loss of productivity. They also use an organization's valuable network resources.

- Websites – A common ploy is to offer something free or a chance to win a sweepstakes on a Website. To win the user must enter an email address and a password. Many employees will enter the same password that they use at work, so the Social Engineer now has a valid user name and password to enter an organization's network.

Policies and Procedures:

Since there is neither hardware nor software available to protect an organization against Social Engineering, it is essential that good policies and procedures be in place to protect against it. Policy is often cited as the first, most critical component to any information security program.

To be successful a good policy must be realistic. It should not contain rules or directives that may be unattainable. They should describe a good control environment while remaining realistic enough to be successful. They should be concise, yet thorough. Policies have a life cycle, and they need to be kept current. A good way to do this is to make them paperless by putting them on the organization's Intranet. This insures that everyone is looking at the latest version of the policy.

Security policies should cover the following areas:

- Account Setup. Procedures should be in place for how new employees will be set up on the system. Equally important are procedures to make sure employees leaving the organization are removed from the system.

- Password change policy. There should be a policy in place to require employees to change their passwords frequently and to use hardened passwords, or passwords that are hard to break. Most password attacks use a form of a dictionary program that uses a dictionary to crack passwords. By including special characters, numbers, misspelled words and double words the user can make their passwords more difficult to crack. Consideration must be given to striking a balance as too how difficult a password is required to be and how often it must be changed. If employees are required to have 16-position passwords and change them weekly, they are very likely to write

them down so they can remember them. This defeats the intended purpose of the passwords.

- Help Desk procedures. There must be a standard procedure for employee verification before the help desk is allowed to give out passwords. A caller id system on the phone is a good start so the help desk can identify where the call originates. The procedure could also require that the help desk call the employee back to verify his location. Another method would be to maintain an item of information that the employee would be required to know before the password was given out. Some organizations do not allow any passwords to be given out over the phone. The help desk must also know who to contact in case of security emergencies.

- Access Privileges. There should be a specific procedure in place for how access is granted to various parts of the network. The procedure should state who is authorized to approve access and who can approve any exceptions.

- Violations. There should be a procedure for employees to use to report any violations to policy. They should be encouraged to report any suspicious activity and assured that they will be supported for reporting violation. If one attempt occurs, it is usually the "tip of the iceberg." Knowing a Social Engineering effort is underway as early as possible can help an organization warn others.

- The organization should have a means of identifying their employees. One way is to require employees to wear picture ID badges. Any guest should be required to register and wear a temporary ID badge while in the building. Employees should be encouraged to challenge anyone without a badge.

- Privacy Policy. Company information should be protected. A policy should be in place stating that no one is to give out any more information than is necessary. Phone surveys are common, and they often ask for information that would be useful to a Social Engineer. A good policy would be to refer all surveys to a designated person. The policy should also contain procedures for escalating the request if someone is asking for more information than the employee is authorized to provide.

- Paper Documents. All confidential documents should be shredded.

- Modems. Modems attached to individual computers are a major security risk because they do not go through the firewall. Policy should not allow any modems attached to a network computer. It is good practice to audit for modems by having some type of War Dialing software available. This software will dial all of the phones in the organization's range of numbers and check for any modems in auto-answer mode.

- Sensitive areas should be physically protected with limited access. Doors should be locked and access only granted to employees with a business need.

- A centralized point should be established to control any information about viruses. This person should verify that any reported viruses are not hoaxes. Established procedures should be in place to take action and prevent the spread of any real viruses.

The Importance of Employee Education:

Good policies and procedures are not effective if they are not taught and reinforced to the employees. It is not enough to just publish the policies and expect employees to read and understand them. They need to be taught to emphasize their importance. After receiving training, the employee should sign a statement acknowledging that they understand the policies.

This training should be part of new employee orientation to the organization so that employees coming to work after the initial training will still be trained. A refresher course should be held periodically to keep the employees up to date on changes to the policies and to reinforce their importance.

Another way to keep employees informed and educated is to have a web page dedicated to security. It should contain any new ploys being reported so the employees will be aware of them. It could also have a "Tip of the Day" to reinforce certain policies.

Summary:

Social Engineering is a serious problem. An organization must establish good policies to guard against it, and these policies must be communicated throughout the organization. It does no good to have firewalls, intrusion detection software and anti-virus software if employees give the key to the door to anyone who asks.

Once established and trained, the policies must also be enforced and supported. If the help desk refuses to give an angry Vice President his password, then the help desk must be supported if the Vice President complains to the employee's management. Also, action must be taken against employees who violate policy to show that management is serious about security.

For Further Information:

4Comm, Inc. "Social Engineering Test." November 1999. URL: http://www.4securedata.com/services/scc4.html. (9 February 2001).

CERT. "CERT Advisory CA1991-04 Social Engineering." 18 September 1997. URL: http://www.cert.org/advisories/CA-1991-04.html. (9 February 2001).

Fennelly, Carole. "The human side of social engineering on Internet security." 01 July 1999. URL: http://www.sunworld.com/unixinsideronline/swol-07-1999/swol-07-security.html. (12 February 2001).

Grefer, Roland and Kolde, Jennifer. (1999). "Security Essentials 2." SANS Institute.

Ryder, Josh. "Preventing Information Loss: Strengthening a Weak Link." Security Portel. 22 August 2000. URL: http://www.securityportal.com/topnews/infoloss20000822.html (9 February 2001).

Shultz, E. Eugene. (2000). Windows NT/2000 Network Security. USA. MacMillian Technical Publishing.

Spernow, William. "What the Help Desk Should Know About Dealing With Potential Security Breaches." Gartner Group. 23 October 2000. URL: http://www4.gartner.com/DisplayDocument?id=314785&acsflg=accessBought.html (9 February 2001).

Vigilante. "Social Engineering." Internet Security. URL: http://www.vigilante.com/inetsecurity/socialengineering.htm (12 February 2001).

Winkler, Ira (1997). Corporate Espionage. California. Prima Publishing.