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.

The Threat of Social Engineering and Your Defense Against It

There are several methods that the malicious individual can use to try to breach the information security defenses of an organization. The human approach, often termed Social Engineering, is one of them. This paper describes Social Engineering and its cost to the organization. It discusses the various forms of Social Engineering, and how they take advantage of human behavior. It also discusses ways to fight and prevent social engineering attacks, and highlights the importance of policy and education in winning the batt...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Radha Gulati
GIAC Security Essentials (GSEC) Certification Practical Assignment
Version 1.4b – Option 1

The Threat of Social Engineering and Your Defense Against It

Abstract:

There are several methods that the malicious individual can use to try to breach the information security defenses of an organization. The human approach, often termed Social Engineering, is one of them. This paper describes Social Engineering and its cost to the organization. It discusses the various forms of Social Engineering, and how they take advantage of human behavior. It also discusses ways to fight and prevent social engineering attacks, and highlights the importance of policy and education in winning the battle.

© SANS Institute 2003, Author retains full rights.

The Threat of Social Engineering and Your Defense Against It

Introduction

Intruders and hackers are on the lookout for ways to gain access to valuable resources such as computer systems or corporate or personal information that can be used by them maliciously or for personal gain. Sometimes they get their chance when there are genuine gaps in the security that they can breach. Often times, in fact more often than one can guess, they get through because of human behaviors such as trust – when people are too trusting of others, or ignorance – people who are ignorant about the consequences of being careless with information. Social Engineering uses human error or weakness to gain access to any system despite the layers of defensive security controls that have been implemented via software or hardware. The ultimate security wall is the human being, and if that person is duped, the gates are wide open for the intruder to take control.

Definition of Social Engineering

Social engineering is the 'art' of utilizing human behavior to breach security without the participant (or victim) even realizing that they have been manipulated.

Categories of Social Engineering

There are two main categories under which all social engineering attempts could be classified – computer or technology based deception, and human based deception.

The technology-based approach is to deceive the user into believing that he is interacting with the 'real' computer system and get him to provide confidential information. For example, the user gets a popup window, informing him that the computer application has had a problem, and the user will need to re-authenticate in order to proceed. Once the user provides his id and password on that pop up window, the harm is done. The hacker who has created the popup now has the user's id and password and can access the network and the computer system.

The human approach is done through deception, by taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked.

For example, the attacker impersonates a person with authority, He places a call to the help desk, and pretends to be a senior Manager, and says that he has forgotten his password and needs to get it reset right away. The help desk person resets the password and gives the new password to the person waiting at

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the other end of the phone. At the very least, the individual can now access the Personnel systems as if he were the manager, and obtain the social Security numbers and other confidential/private information of several employees. He could of course do more damage to the network itself since he now has access to it.

Impact of Social Engineering on the organization:

Information Security is essential for any organization 'to continue to be in business'. If information security is not given priority, especially in the current environment with the threat of terrorism looming in the background every day, even a small gap in security can bring an organization down.

The financial cost could be punitive to the organization and to the individual. So much so, that insurers are now beginning to cover losses arising out some kinds of security breaches[1].

Cyber attacks cost U.S. companies $266 million last year - more than double the average annual losses for the previous three years, according to a report released by the San Francisco-based Computer Security Institute (CSI) and the San Francisco FBI Computer Intrusion Squad. The study found that 90% of 273 respondents detected some form of security breach in the past year. But this is probably an underreported figure. Less than half the companies in one survey were willing or able to quantify the loss[2].

There is also the cost of loss of reputation and goodwill, which can erode a company's base in the long run**.** For example, a malicious individual can get access to credit card information that an online vendor obtains from customers. Once the customers find out that their credit information has been compromised, they will not want to do any more business with that vendor, as they would consider that site to be insecure. Or they could initiate lawsuits against the company that will lower the reputation of the company and turn away clientele.

Something similar happened with PayPal, the online payment company. PayPal customers received email that asked the account holder to re-enter their credit card data. PayPal purportedly had had some trouble with one of its computer systems. The e-mails looked like the genuine article, with PayPal logos and typefaces, even the security lock symbols and a link that resembled the official PayPal link. When accountholders provided the information, the hacker was able to harvest it[3].

---

[1] Hoffman, Thomas. "Premium Protection: Security Breaches. Viruses. Should you amend your IT insurance plan to cover such risks?" Computerworld March 31, 2003

[2] Harrison, Ann. "Survey: Cybercrime Cost Firms $266M in 1999". Computerworld March 27, 2000.

[3] Rosencrance, Linda. "Online Payment Service PayPal hit by scam". Computerworld, September 27, 2002.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Security experts concur when it comes to identifying where security violations can occur, and who causes them. Over time, the experts have come to the conclusion that despite the impression of the hacker being an outsider wanting to get 'in', the majority of violations are caused by either disgruntled employees or non-employees who have legitimate system access because of their job in the organization. According the FBI nearly 80% of all attacks are caused by such authorized users[4].

In most cases, once the individual is wearing the cloak of respectability, others do not automatically view their activity with suspicion: every honest person assumes that others are similarly well intentioned. The intruder also takes advantage of the natural tendency to relax one's guard when things appear to be secure.

In short, companies spend billions of dollars every year in improving hardware and software in order to block malicious attacks. But all this is of no use if end users do not follow good security practices[5].

From an interview of Kevin Mitnick, an infamous hacker in the 1980s and 1990s, with the BBC News Online [6]:

> The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you.
>
> What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time organizations overlook that human element.

Common techniques used in Social Engineering

Direct approach

> It is 8 pm on Friday evening, and Employee A is working on resolving a critical problem in the Personnel computer system, and is called away by an emergency at home. Employee B, who has been upset with his manager, offers to help out, and work on the problem. However B does not have access to the system, and there is no time to go through the proper channels to request the access for B. So A gives B his ID and

---

[4, 5] National Security Institute's (www.nsi.org) online 'Employee Information Awareness Service' web page content as of August 2003. URL: http://nsi.org/SSWebSite/TheService.html

[6] Mitnick, Kevin, "How to Hack People." BBC NewsOnline, October 14, 2002.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

password, without realizing that B has an ulterior motive in offering to help. When A is fighting fires at home, B has access to the network, the database and anything else that A has access to. B can now do what he wishes, and even better, he can do it without having his identity revealed in the process.

Or take the very common security problem of tailgating. Joe, who has forgotten his passkey into the building, shadows Barb as she 'keys in', and slips in after her. Often Barb does not know Joe, or even notice that Joe has tailgated after her. And more often than not, even if Barb has noticed, she will not turn around and stop Joe from tailgating. She would not feel comfortable doing that, as it might create a scene in front of others. If Joe is an intruder, he has achieved the first step in his plan - he has gained physical access into the premises.

Dumpster Diving

Who ever would have that that throwing away junk mail or a routine company documents without shredding, could be threat? But that is exactly what it could be, if the junk mail contained personal identification information, or credit card offers that a 'dumpster diver' could use in carrying out identity theft. The unsuspecting 'trash thrower' could give the Dumpster Diver his break.

Company phone books and organization charts provide phone numbers and locations of employees, especially management level employees who can be impersonated to the hacker's benefit.

Procedure and policy manuals can help the hacker to become knowledgeable about the company's policies and procedures, and thus be able to convince the victim about their authenticity.

Calendars are an important source of information about meetings, vacation etc, that the hacker can use to improve his 'storyline' when deceiving the unsuspecting secretary.

In his interview with the BBC News Online, Kevin Mitnick explains, 'how armed with a little knowledge, a hacker can sound like an employee of a firm and get other workers to inadvertently supply them with enormously useful information' [7].

The hacker can use a sheet of paper with the Company letterhead to create official looking correspondence.

[7] Mitnick, Kevin, "How to Hack People." BBC NewsOnline, October 14, 2002

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A hacker can retrieve confidential information from the hard disk of a computer. There are ways to retrieve information from disks, even if the user thinks the data has been 'deleted' from the disk.

Spying and eavesdropping

A clever spy can determine the id and password by observing a user typing it in. All he needs is to be there behind the user and be able to see his fingers.

If the policy is for the helpdesk to communicate the password to the user via the phone, then if the hacker can eavesdrop or listen in to the conversation, the password has been compromised.

An infrequent computer user may even be in the habit of writing the id and password down, thereby providing the spy with one more avenue to get the information.

Technical expert

Take the case where the intruder posing as a support technician working on a network problem requests the user to let him access her workstation and 'fix' the problem. The unsuspecting user, especially if she is not technically savvy, will probably not even ask any questions, or watch while her computer is taken over by the so called technician. Here the user is trying to be helpful and doing his part in trying to fix a problem in the company's network.

Support staff

How many people would suspect a member of the janitorial staff could hack into the network? A man dressed like the cleaning crew, walks into the work area, carrying cleaning equipment. In the process of appearing to clean your desk area, he can snoop around and get valuable information – such as passwords, or a confidential file that you have forgotten to lock up, or make a phone call impersonating you from your desk.

Or take the case of the deceptive telephone repairman. The intruder can pose as a repairman and walk up to your phone and fiddle around with the instrument, and the wiring etc, and in the process spy on your workplace for valuable information that has been left unsecured.

The voice of Authority

The attacker can call up the company's computer help desk and pretend to have trouble accessing the system. He claims to be in a very big hurry,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and needs his password reset immediately and demands to know the password over the phone. If the attacker adds credence to his story with information that he has picked up from other social engineering methods, the help desk personnel is all the more likely to believe the story and do as requested.

The Trojan horse

Like the Trojan horse from Greek mythology, the attacker can cause by sending what appears to be harmless email to random recipients.

One kind of attack is done when the attacker sends an innocuous email attachment that the unsuspecting victim opens, and thereby launches a virus or a worm, which can eventually infect the entire network. The 'I Love You' virus and the 'Anna Kournikova' worm are examples of these.

The other kind of attack that targets the user in a similar way is the chain-mail email that promises a reward if the recipient forwards it on to n number of people and a dire outcome otherwise. This appears to be a harmless way to invite good fortune, and the recipient is often tempted to do as suggested. But the result is an exponential load on the network resources, and can bring the network down.

The popup window

The attacker's rogue program generates a pop up window, saying that the application connectivity was dropped due to network problems, and now the user needs to reenter his id and password to continue with his session. The unsuspecting user promptly does as requested, because he wishes to continue working, and forgets about it. Later he hears that there has been an attack on the system, but never realizes that that he was the one who opened the gate!

Behaviors vulnerable to Social Engineering attacks

All the Social Engineering methods of attack target some very natural human attributes. These are listed below along with the Social engineering tactics that target them

- Trust (Direct approach, Technical expert)
- The desire to be 'helpful' (Direct Approach, Technical expert, Voice of Authority)
- The wish to get something for nothing (Trojan horse - chain email)
- Curiosity (Trojan horse - open email attachments from unknown senders)
- Fear of the unknown, or of losing something (Popup window)
- Ignorance (Dumpster diving, Direct Approach)
- Carelessness (Dumpster Diving, Spying and eavesdropping)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Measures to reduce the impact

- A well documented and accessible Security Policy
- Training on Security Policy
- Awareness of threats and impact of social engineering on the company
- Implement and audit policy usage
- Identity Management policy
- Operating procedures to limit vulnerabilities.
- Use of physical technical solutions 'intelligent revolving doors', biometric systems, to eliminate or reduce unauthorized physical access
- Cost mitigation with insurance protection

Security Policy

A well-documented and accessible Security Policy and associated standards and guidelines form the foundation of a good security strategy. The policy should clearly document in layman terms, its scope and content in each area that it applies to. Along with each policy, should be specified the standards and guidelines to be followed in order to comply with the policy.

For example, the policy should cover

- Computer system usage – monitoring usage, the use of non Company-standard hardware or software, response to chain mail etc,

- Information classification and handling – to ensure that confidential information is correctly classified as such, and it is secured and disposed of properly. Compliance would result in environment and network information being secured, and not easily available to everybody.

- Personnel security – screening new and non employees to ensure that they do not pose a security threat

- Physical security – to secure the facility via sign in procedures, electronic and biometric security devices etc, and to through

- Information access – password usage and guidelines for generating secure passwords, access authorization and accountability, remote access via modems etc

- Protection from viruses – to secure the systems and information from viruses and other threats

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Information security awareness training and compliance – to ensure that employees are kept informed of threats and counter measures

- Compliance monitoring – to ensure that the security policy is being complied with.

- Password policies - standards for secure passwords should be defined. Passwords should be required to expire after a specified period in all systems.

- Documentation retention and destruction. For example all confidential information should be disposed of by shredding, not by discarding in the trash or recycle bins.

Once the policy is documented, it needs to be made easily available to everyone in the organization. This could be best accomplished by publishing it on the company's intranet and having links to it from the home page and other major pages on the intranet.

Education

For the policy to be effective, Education must be a regular feature. Some companies require all employees review the policy each year, to acquaint themselves with revisions if any. All new employees and non-employees MUST be trained as soon as they start with the company.

Awareness of threats and risky behavior

Building awareness of the methods employed and behaviors targeted by the information bandit is an important part of the defense strategy. Educating employees on the damage done by such theft is also a must. The best way to create such awareness in the general non-security professional, is through real life examples of companies have been hacked because of insider information, or even just negligence and ignorance on an employee's part.

There are organizations that contract to provide this content. The identity of the hacked companies is of course kept secret. The stories are updated regularly, such as once a month. All you need to do, is to provide a link to the website where the stories are published. Alternatively, in order to make the experience more proactive, as a user logs on each day, a window could come up, with the 'attack' or 'defense' of the day story.

Audit Policy usage and compliance

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Having created the policy and educated the user is not enough, if no one conforms to the policy. Hence there is a need to audit the usage across the enterprise.

For example, when a project is going through quality assurance, it should also go through security policy compliance verification. Audit procedures must be in place, to verify for example that the help desk person is not communicating passwords over the phone or via unencrypted email.

Periodically Managers should review the access of their employees. Security audits should confirm that employees who no longer need access do not have access.

Access points such as entry doors etc should be routinely monitored. This will ensure that employees are complying with policy regarding access to secured locations.

Employee workspaces should undergo random inspection to ensure that confidential material is always secured in locked cabinets. Workstations should be locked down and password protected screensavers should be in use.

Identity Management

It is common for organizations to have a unique identifier for each employee. This is often used as their ID to access all computer systems, and also as the key identifier for the individual in the organization. For example the company assigns a 5 character Employee ID to each employee the day they get hired. This ID is unique to each employee, and is the key to all Personnel data. Since this ID uniquely identifies the employee, it is also assigned as the Sign on ID in all the computer applications that the employee has access to.

The inherent risk in using this ID for ALL identification purposes is that once the intruder finds out Bob's employee ID, he can use that to get access to network and computer applications that Bob has access to. His work of hacking into the system has been cut in half. He only has to find Bob's password to the system, not the ID itself.

However, keeping the base for personnel identification distinct from that used for computer systems can mitigate this risk. It may mean some additional work, but it will help to limit the damage from an attack.

Operating Procedures

Standard operating procedures, especially those related to providing security access or clearance, should have a cross verification or 'call back' step before

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the request is granted. This will reduce the number of times the hacker can get away with trying to impersonate a legitimate user.

Insurance Protection

Finally, an organization can buy insurance against security attacks. However most insurers will look for company policies and procedures that work towards reducing the threat of attacks. Examples of these are:

- The internal audit policies
- Password policies
- HR hiring policies with regard to background checks
- Security awareness and education programs and compliance requirements for employees and non employees
- Contracts with vendors and other external providers

Insurers are "not so much concerned with the products [customers] are using to mitigate attacks" as they are "with the [employee and access] controls and policies they've put in place" [8].

Summary

Social Engineering is the way an intruder can get access to your information resources without having to be a technical, network or security expert. The attacker can use many tactics to either fool the victim into providing the information he needs to gain entry, or obtain the information without the victim's knowledge. The cost of failing to eliminate social engineering attacks is very high.

Good Information Security strategy is a critical component of an overall strategy to ensure the success of the organization.

The organization can reduce the impact of Social Engineering attacks by implementing a comprehensive information security strategy. Such a strategy would include measures ranging from publishing a well written security policy, implementing ongoing security awareness and education programs, following through with auditing programs to monitor policy compliance, installing security devices to prevent unauthorized physical access and buying insurance against security attacks.

[8] Hoffman, Thomas. "Premium Protection: Security Breaches. Viruses. Should you amend your IT insurance plan to cover such risks?" Computerworld March 31, 2003

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References:

1. Hoffman, Thomas. "Premium Protection: Security Breaches. Viruses. Should you amend your IT insurance plan to cover such risks?" Computerworld March 31, 2003.
   URL: http://www.computerworld.com/securitytopics/security/story/0,10801,79794,00.html (Aug 12, 2003)

2. Harrison, Ann. "Survey: Cybercrime Cost Firms $266M in 1999." Computerworld March 27, 2000
   URL: http://www.computerworld.com/news/2000/story/0,11280,44243,00.html (Aug 12, 2003).

3. Rosencrance, Linda. "Online Payment Service PayPal hit by scam." Computerworld, September 27, 2002.
   URL: http://www.computerworld.com/securitytopics/security/story/0,10801,74687,00.html (Aug 12, 2003).

4. National Security Institute (www.nsi.org). Employee Information Awareness Service. August 2003.
   URL: http://nsi.org/SSWebSite/TheService.html (Aug 12, 2003).

5. Mitnick, Kevin. "How to Hack People." BBC NewsOnline, October 14, 2002.
   URL: http://news.bbc.co.uk/1/hi/technology/2320121.stm (Aug 12, 2003).

6. Winkler, Ira S. and Dealy, Brian. "Information Security Technology? …Don't Rely on It. A Case Study in Social Engineering."
   URL: http://www.usenix.org/publications/library/proceedings/security95/winkler.html (Aug 12, 2003).

7. Stevens, George. "Enhancing Defenses against Social Engineering". GIAC Practical Repository.
   URL: http://www.giac.org/practical/gsec/George_Stevens_GSEC.pdf (Aug 12, 2003).

8. Evenson, Jake. "Social Engineering: A Way Around the Hardware". GIAC Practical Repository.
   URL: http://www.giac.org/practical/GSEC/Jake_Evenson_GSEC.pdf (Aug 15, 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

9. Gilhooly, Roger. “The Social Approaches to enforcing Information Security”. Sans Reading Room, December 11, 2002.
URL: http://www.sans.org/rr/paper.php?id=1102 (Aug 12, 2003)

10. Arthurs, Wendy. “A Proactive Defense to Social Engineering.” SANS Reading Room, August 2, 2001.
URL: http://www.sans.org/rr/paper.php?id=511 (Aug 12, 2003).

11. Sullivan, Brian. “Getting Hurt by What You Don’t Know”. ComputerWorld, January 11, 2001. URL:
http://www.computerworld.com/securitytopics/security/story/0,10801,67319,00.html (Aug 12, 2003).

12. Granger, Sarah. “Social Engineering Fundamentals, Part I: Hacker Tactics.” Security Focus, December 18, 2001.
URL: http://www.securityfocus.com/infocus/1527 (August 12, 2003).

13. Memory, Bev. “Security Awareness – Everyone’s Business”. GIAC Practical Repository.
URL: http://www.giac.org/practical/gsec/Bev_Memory_GSEC.pdf (Aug 15, 2003).

14. Allen, Malcolm. “The Use of Social Engineering as a means of Violating Computer Systems.” SANS Reading Room. October 12, 2001.
URL: http://www.sans.org/rr/social/violating.php (Aug 15, 2003).

15. Gragg, David. “A Multi-Level Defense against Social Engineering.” SANS Reading Room, March 13, 2003
URL: http://www.sans.org/rr/paper.php?id=920 (Aug 12, 2003).

16. Heuer, Richard J. “Theft and Dumpster Diving”
URL: http://www.mbay.net/~heuer/T3method/Theft.htm (Aug 12, 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 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**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**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**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 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**