The Use of Social Engineering as a Means of Violating Computer Systems; Hacker Tactics, Combat Strategies and The human firewall

Owolabi Animashaun
Department of Information Science and Technology
Universiti Kebangsaan Malaysia
Bangi, Malaysia
oanimashaun@gmail.com

Abstract

From a management perspective, a social engineering attack can be frustrating and difficult to identify. As organizations continue to battle against computer hackers, the focus continues to be on technology defenses. The con artist, or social engineer, hacks with a focus on employees rather than computers. As organisations scramble to put an end to network infiltration, social engineers turn to infiltrating people. Infact, social engineers/hackers have accomplished some of the largest, vicious and unbelievable security breaches and terrorist attacks in history. Organizations are targeted through social engineering as it is often an easier way to gain illegal access than many other forms of technical hacking. Almost all big organizations and even government parastatals are not left out of this deadly attack made possible by skilled human deception. This paper is written to review the current state of this threat and increase the awareness of organizations as regards social engineering.

1. Introduction

Social engineering is the use of non-technical means to gain unauthorized access to information or computer systems. It is a hacker term for deceiving people into revealing confidential information. It is a tactic that is often used by hackers to gain information about a network or simply to bypass a complex security system altogether. It is a hackers clever manipulation of the natural human tendency to trust, with the goal of obtaining information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system. 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 or simply disrupt the system or network, identity theft or even industrial espionage. It is increasingly becoming recognized as a major threat in the Computer Industry as evidenced by a report by the Institute of Management and Administration (IOMA) in the US that this form of security violation is on the rise due to continued improvements in technical protections against hackers. Infact, it is regarded as the greatest security threat of the next decade. Organizations spend a lot of money and time trying to protect their networks; they focus their attention mostly on technology such as upgrades, security devices, laying out firewalls, putting routers that filter packets and filter IP addresses, they are even installing better login authentication systems but a popular means of gaining access bypasses the technical systems completely. It is based on the long-time con-game but has a new name and face; social engineering. An organization needs good policies in place but even more, they need an effective, on-going security awareness program to protect against this type of attack. The best means of defense, in this case, is education. For the hacker, it is an essential skill that can be used to bypass even the most sophisticated security measures without even being detected. Social engineering is a hackers clever manipulation of the natural human tendency to trust, with the goal of obtaining information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system. Social Engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone but through an effective, on-going security awareness program and educating employees to follow the policies.

2. HACKER TACTICS

In general, Social Engineering is the criminal art of scamming or deceiving people into giving confidential, private or priviledged information or access to a hacker. There are just a few differences between the techniques used for social engineering and that used to carry out a traditional hacking; both aim at gaining 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. Social engineering attacks take place on two levels: the physical and the psychological. The physical setting for these attacks could be; the workplace, the phone, dumpster or trash, and even on-line. In the workplace, the hacker can simply walk in the door and pretend to be a maintenance worker or consultant who has access to the organization. Then the intruder walks through the office until he or she finds a few passwords lying around and emerges from the building with enough information to exploit the network from anywhere. Another technique to gain authentication information is to just stand there and watch an oblivious/unknowing employee type in his/her password. Social engineers mix old and new methods to grab passwords or profits. Being aware of their tricks is the first line of defense. Below are some of the tactics commonly used by social engineers:

1. On-Line Social Engineering The Internet is a very good medium for social engineers looking to harvest passwords. The primary weakness is that many users often repeat the use of one simple password on every account: yahoo, google, hotmail, facebook, linked even on extremely sensitive areas such as bank account. Once a hacker gets access to one account, he/she automatically has access to all the other accounts. One way in which hackers commonly obtain this kind of password is through an on-line/e- form: they write a program or edit one that is already written to request usernames and passwords in exchange for a grand price, these forms are usually sent through the e-mail. Hackers can also use news against you by using such information as social engineering lures for spam, phishing and other scams. For instance they could send you an email saying; Your bank is being bought by this another bank. Please click here to make sure you update information before the sale closes.' It's an attempt to get you to release your information so they can log into your account to either steal your money or sell your information to someone else. Or; this site is undergoing maintenance, click here to update your information. Of course, when you click on the link, you go to the hackers site Another way social engineers may obtain information on-line is by pretending to be the network administrator thereby sending e-mails through the network and asking for a users password. This type of social engineering attack does not usually work because users are generally more aware of hackers when online, but it is something of which to take note. In addition, pop-up windows can be installed by hackers to look like part of the network and request that the user reenter his username and password to fix some sort of problem. At this point in time, most users should know better than to send their passwords to anybody or any site in clear text (if at all), but it is always better to have a reminder of this simple security measure from the System Administrator.

2. Abusing faith in social networking sites Facebook, tagged, twitter, Linked- these are all hugely popular social networking sites. Many people have a lot of faith in them and generally believe they are safe; social engineering wise. Increasingly, social networking devotees are being fooled by emails that claim to be from sites like Facebook but are really from scammers. A recent spear-phishing incident targeted Linked In users, and the attack was surprising to many. As it was extremely successful and unexpected by many.

3. Dumpster Diving This is also known as trashing. It is the practice of rummaging through the trash to find useful scraps of information that have been discarded. The social engineer collects as much trash as possible without being noticed. A huge amount of information can be collected through this way. Many items such as company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware are potential security leaks and must be securely monitored to the point of destruction. For example; phone books can give the hackers names and numbers of people to target and impersonate. Calendars may tell attackers which employees are out of town at a particular time and impersonate such employees. Organizational charts contain information about people who are in positions of authority within the organization. System manuals, sensitive data, and other sources of technical information may give hackers the exact keys they need to unlock the network. Memos provide small tidbits of useful information needed for creating authenticity. Policy manuals show hackers the policy of the company(this is meant to be very private) and how secure or insecure the company really is. Finally, outdated hardware, particularly hard drives, can be restored to provide all sorts of useful information.

4. Phone-number spoofing Social Engineers also use phone-number spoofing to make a different number show up on the target's caller ID. Social Engineering by phone is the most prevalent type of social engineering attack. The hacker could actually be sitting in his/her apartment calling you, but the number that shows up on the caller ID appears to come from within the company. A hacker will call up and imitate someone in a position of authority or reverence in the company and gradually pull information out of the victim. Help desks are particularly prone to this type of attack. Hackers are able to pretend they are calling from inside the corporation by playing tricks on the PBX or the company operator. A lot of unsuspecting victims usually give private information, like passwords over the phone if the caller ID legitimizes it. And, of course, the crime is often undetectable or untraceable later because if you dial the number back, it goes to an internal company number.

5 Learning your corporate language Successful social engineering needs detailed planning, time, persistence and patience as attacks are often done slowly and methodically. This build-up includes collecting personal tidbits about people and also collecting other ”social cues” to build trust and even fool other people into thinking they are an employee

when they are not. Every industry has a short hand, a social engineering criminal will study that language and be able to use it like any member of staff during his act. It will be so convincingly done that even the most senior management staff could fall for it and fall prey to the hacker. Another successful technique involves recording the ”hold” music a company uses when callers are left waiting on the phone. The criminal gets put on hold, records the music and then uses it to his/her advantage. When he or she calls the intended victim, they talk for a minute and he then says ”Oh, my other line is ringing, hold on,” and put them on hold. ”The person being scammed hears that familiar company music and thinks: ’Oh, he must really be a staff of our company. That is our music. This is just another psychological cue to lure the unknowing victim.

6. Typo Squatting On the internet, social hackers bank on the common mistakes people make when they type. When a wrong URL is typed that is just one letter off, suddenly you can end up with unintended consequences. Social engineers are prepared for typing mistakes and the site they prepare looks a lot like the site unsuspecting users thought they were going to. Instead of going where they wanted, unsuspecting users who make typing mistakes end up on a fake site that either intends to sell something, steal something, or push out malware.

7. Reverse Social Engineering A more advanced method of gaining illicit information is known as reverse social engineering. This is when the hacker causes a problem on the target network or computer and then makes himself/herself available to fix the problem. Once the hacker fixes the problem, he/she has gained the confidence and trust of the target as he is perceived as a hero. He then requests certain bits of information from the victims and gets what he really came for. They never know it was a hacker, because their network/computer problem goes away and everyone is happy. For reverse social engineering to be successful, the hacker has to be able to get onto the target computer or system ahead of time or possible send a file to cause the originating problem. However, this requires a great deal of preparation, research, and pre-hacking to pull off.

8. Using FUD to affect the stock market : The social engineer uses the old fear, uncertainty and doubt(FUD) of security and vulnerabilities of products, and even entire companies to affect the equities market. The method is to use email to execute the ancient ’pump-and-dump’ tactic. A scammer buys a large volume of a penny stock, then send out emails under the guise of an investment advisor touting that stock’s great potential (that’s the ’pump’). If enough recipients of this spam email rush to buy the stock, the price will automatically rise upward. The scammer then quickly ’dumps’ his shares at a great profit.

9. CD/USB dropping: An easy tactic that can be used to obtain sensitive information or remote access to a targets computer. The social engineer drops off a CD (USB key) with malicious software in a high traffic area such as the front desk or toilet. The USB/CD is labeled with a an important title like layoff list. As most staff will be interested in finding out about this, they quickly pick up the CD/USB inserts into the system thereby unknowingly allowing the malicious software in this CD,USB to run using the auto run feature or it will run when the user clicks an executable file. The malicious software could potentially open a back door into the victims computer without their knowledge, allowing the social engineer to execute attacks from this recently compromised host.

3. Spotting a Social Engineering Attack

To foil attack employees should be able to recognize it as such. Some signs of social engineering attacks to recognize are: requesting forbidden information, refusal to give contact information, rushing, name-dropping, intimidation and small mistakes (misspellings, misnomers, odd questions). Also, employees are implored not to be overly helpful as always be logical by looking for things that dont quite add up as to understand the enemy, one must think like him. Companies can help to ensure security by conducting ongoing security awareness programs. Organizational intranets can be a valuable resource for this approach, particularly if on-line newsletters, e-mail reminders, training games, and strict password changing requirements are included. The biggest risk is that employees may become complacent and forget about security. Continued awareness throughout the organization is the key to ongoing protection - some organizations even create security awareness programs, such as the distribution of trinkets mentioned above.

4. COMBATTING SOCIAL ENGINEERING

Building a defense against social engineering is similar to building any strong defense. The catch is to determine what and where the vulnerabilities are and then defend against them. Since social engineering has been so successful, there is a need for a critical combat strategy. Below are some of some ways that individuals and organizations can protect themselves against potentially costly social engineering attacks.

1. Strong Security Policies: Many organizations make the mistake of only planning for attack on the physical side. This leaves them wide open from the social-psychological angle. As such, senior management must understand the importance of developing and implementing well-rounded security policies and procedures as all of the money spent on software patches, security hardware, and audits will be a waste without adequate prevention of social engineering and reverse social engineering attacks. The policies must not be too general or specific as it should give policy enforcers some flexibility in how procedures will develop

in the future, but limits staff from becoming too relaxed in their daily practices. The end use must not be in the position where they have to determine if certain information should be given out or not. The security policy should address information access controls, setting up accounts, password changes, access approval and even escorting of visitors. Modems should never be permitted on the company intranet. Locks, IDs, and shredding should be required. Discipline must be built in, enforced and violations should be posted and prosecuted.

2. Security Awareness Training and Retraining: In order to be successful, organizations must make computer security part of all jobs, regardless of whether the employees use computers or is at the help desk or not. Security awareness is more complicated than just telling people not to give their password, PIN or Login ID away. Employees must know what kind of information a social engineer can use and what kind of information is suspect. Everyone in the organization needs to understand exactly why it is so crucial for the confidential information to be designated as such, therefore it benefits organizations to give them a sense of responsibility for the security of the companys information. All employees should be aware of the basic signs present in a social engineering attack. They must be able to say No when it is appropriate and have the backing of their management on the occasions when it might be offensive. Employees should know what have values, passwords and login PINs are personal, friends are not always friends, uniforms can be bought or had by anyone and there is no trusting anyone with the companys private information. All employees should be trained on how to keep confidential data safe. Get them involved in the security policy. To reduce risk and educate staff, the awareness session should be presented in a friendly environment where no one is reprimanded or singled out. All project staffboth internal employees and consultantsshould be invited to the presentation. All newly employed employees MUST go through a security orientation progarm and the old staff kept informed via videos, newsletters, brochures, booklets, signs, posters, coffee mugs, pens and pencils, printed computer mouse pads, screensavers, logon banners, notepads, desktop artifacts, T-shirts and stickers so as to remind them constantly of the threat of social engineering. I

3. Preventing Physical Attacks : Anyone who enters the organizations premises should have his/her ID card checked and verified. There should be no exception to this. Important documents need to be physically locked in file drawers or other safe storage sites and their keys not easily accessible to all and sundry. Other documents may require shredding especially if they ever go near the dumpster. Also, all magnetic media should be bulk erased as data can be retrieved from formatted disks and hard drives. Waste bins and dumpsters should be locked in secure areas that are monitored by security. In the building itself, all machines on the network (including remote systems) MUST be protected by properly implemented passwords and login IDs. Screen saver passwords are also recommended. PGP and other encryption programs can be used to encrypt files on hard drives for further security.

4. Resistance Training for Key Personnel: Key personnel such as help desk personnel, customer service, client service officers, secretaries, receptionists and system administrators/engineers must be given resistance training help prevent them from being persuaded to giving away any information a hacker might need. Resistance training generally hardens people to persuasion. This training should be extended to any employee whose job is to assist others particularly the general public.

5. Incident Response: Organizations need to have a very fast incident response process in place as there is need for a well-defined process that an employee can begin as he/she suspect/detect something is wrong.. This process should immediately inform other potential victims and aggressively go after the hacker. If there is no incident response, every staff that deals with a hacker is fighting a new battle meanwhile the hacker gets more better at understanding the organizations defenses hence , the weaknesses. In all there needs to be a person or department responsible for tracking these incidents preferably a member of the Incident Response Team (IRT), if the organization has one. Employee should notify others who serve in similar positions as they may be threatened as well. From there, the IRT or individual in charge of tracking (a member of the security team and/or system administrator) can coordinate an adequate response so that every attack could be immediately characterized and effectively dealt with.

5. Conclusion

Social engineering is a very real threat that most organizations do not really count as a major threat. The threat is even more real than most network holes; as such organizations needs to take this threat more seriously. However, organizations do not need to create militant staff; just smart and reasonable ones. It is possible to keep morale high and have a fun company culture without sacrificing security. By slight changes and adjustments in the rules of the game, the intruders can be sent packing.

References

[1] Ameritech Consumer Information Social Engineering Fraud, http://www.ameritech.com/content/0,3086,92,00.html

[2] Insiders Pose The Biggest Threat to Data Security CSO Focus Vol.2 No.1 October http://www.cio.com/sponsors/100105$_vontu.pdf Mckeown, KevinwithSter$

[3] Arthurs, Wendy: A Proactive Defence to Social Engineering, SANS Institute, August 2, 2001. http://www.sans.org/infosecFAQ/social/defence.htm

[4] Orr, Chris Social Engineering: A Backdoor to the Vault,, SANS Institute, September 5, 2000 http://www.sans.org/infosecFAQ/social/backdoor.htm

[5] Stevens, George: Enhancing Defenses Against Social Engineering SANS Institute, March 26, 2001 http://www.sans.org/infosecFAQ/social/defense$_{s}ocial.htmBerg, Al : AlBergCrackingaSocialEngineer, by, LANTimesNov.6, 1995.http : //packetstorm.decepticons.org/docs/social - engineering/soc_{e}ng2.html$

[6] Nelson, Rick: Methods of Hacking: Social Engineering, the Institute for Systems Research, University of Maryland http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html

[7] Bernz 1: Bernzs Social Engineering Intro Page http://packetstorm.decepticons.org/docs/social-engineering/socintro.html

[8] Bernz 2: The complete Social Engineering FAQ! http://packetstorm.decepticons.org/docs/social-engineering/socialen.txt

[9] Harl People Hacking: The Psychology of Social Engineering Text of Harls Talk at Access All Areas III, March 7, 1997. http://packetstorm.decepticons.org/docs/social-engineering/aaatalk.html

[10] Mitnick, Kevin: My first RSA Conference, SecurityFocus, April 30, 2001 http://www.securityfocus.com/news/199

[11] Palumbo, John Social Engineering: What is it, why is so little said about it and what can be done?, SANS Institute, July 26, 2000 http://www.sans.org/infosecFAQ/social/social.htm

[12] Stevens, George: Enhancing Defenses Against Social Engineering SANS Institute, March 26, 2001 http://www.sans.org/infosecFAQ/social/defense$_{s}ocial.htmVerizonPBXSocialEngineeringScam2000http : //www.bellatlantic.com/security/fraud/pbx_{s}cam.htm$