IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 5, May 2019

Social Engineering

Alok A Chauhan[1], Nischal Puri[2], Yogesh Narekar[3]

Assistant Professor, Department of IT, RGCER, Nagpur, Maharashtra, India[1,3]

Assistant Professor, Department of IT, PIET, Nagpur, Maharashtra, India[2]

Abstract: The age old problem of social engineering is still a threat that does not receive due attention. Due to the advancements in information technology and the explosion of the Internet, attackers have many more avenues to pursue social engineering attacks. Inadequate efforts to educate employees and staff about social engineering and password management, inappropriate usage of messaging systems, poor implementation and awareness of security policies, all lead to people being exposed to potential incidents. This paper talks about social engineering and the new avenues that it has diverged into; and how social engineering plays a part in assisting other attack schemes. The paper first introduces the concept of social engineering It then looks at different attack methods that have proliferated due to the help obtained by social engineering schemes. Social engineering, both with its low cost and ability to take advantage of low technology, has taken its place in the information security literature as a very effective form of attack

Keywords: Impersonating staff, Hoaxing, Creating confusion, Dumpster diving, Reverse social Engineering

I. INTRODUCTION

As it is well known, only a small percentage of information security is maintained by technical security measures , while its greater percentage depends on the user . Individuals in charge of information security in an organization are all of the organizational staff, with the foremost being the owner of the information and the IT personnel. About seventy percent of information theft is carried out consciously or unconsciously from within the organization. The weakest link. in most of the cases, is unfortunately men When an organization suffers from poor information security , the organization may face the following problems

The information may be collected by others.

- The organization's honor and its image in the society may get damaged (which is the worst case scenario).
- The hardware, software, data and organizational staff may suffer damages.
- Problems of inability to have timely access to important data may arise.
- Monetary losses may occur (the most insignificant part of the problem from a relative point of view).
- Time losses become inevitable.
- There may even be loss of life.

1] shows a distribution , classified by their types, of computer - related incidents that have occurred in the United States of America between the years 2001and 2009.
The graph in [1] shows that stolen laptops occupy the first place with a rate of 21 %, computer hacking occupies the second place with a rate of 16%, web occupies the third place with a rate of 13% , and fraud occupies the fourth place with a rate of 8% . If we classify the hat follow. attacks made using social engineering techniques under the titles of "Computer Hacking" and "Fraud", these incidents form an important portion of crimes with a rate of 24 % in the USA.

II. TYPES SOCIAL ENGINEERING SKILLS

Following are the few Skills to exploits user to get access to your system.

1. Impersonating staff: This is an art of inventing scenario to persuade a target to release information or perform an action and is usually done through email or telephone. Most powerful and danger trick for gaining physical access to the system is to pretend to be someone from inside the company. Users gave their password to a "stranger" on a phone call to a member of the IT staff. This is especially true if the caller implies that their account may be disabled and that they might not be able to get important e-mail or access needed network shares if they don't cooperate[3] . It is the most time consuming attack as it requires research to get information regarding target to establish the legitimacy in the mind of target.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 5, May 2019

2. Playing on users' sympathy the social engineer may pretend to be a worker from outside, perhaps from the phone company or the company's Internet service provider [2]. Nature of people is to help a person who's in trouble.

3. Intimidation tactics social engineers may need to turn to stronger stuff: intimidation. In this case, the social engineer pretends to be someone important -- a big boss from headquarters, a top client of the company, an inspector from the government, or someone else who can strike fear into the heart of regular employees. He or she comes storming in, or calls the victim up, already yelling and angry. [2] They may threaten to fire the employee they don't get the information they want.

4. Hoaxing: A hoax is an attempt to trick the people into believing something false is real. It also may lead to sudden decisions being taken due to fear of an untoward incident

5. Creating confusion: Another ploy involves first creating a problem and then taking advantage of it. It can be as simple as setting off a fire alarm so that everyone will vacate the area quickly, without locking down their computers. Social engineers can then use a logged-on session to do their dirty work. [2]

6. Dumpster diving: Someone from the company throwing away junk mail or routine mail / letter of the company without ripping the document. If the mail contained personal information, or credit card offers that dumpster diver could use to carry out identity theft. Dumpster diver also searches for information like company organization chart, who reports to worm, especially management level employee who can be impersonated to hack important detail. Dumpster diving information can be used in impersonation attack.

7. Reverse social Engineering: An even sneakier met hod of social engineering occurs when a social engineer gets others to ask him or her quest ions instead of questioning them. These social engineers usually have to do a lot of planning to pull it off, placing themselves in a position of seeming authority or expertise

8. Mail: The use of an interesting subject line triggers an emotion that leads to accidental participation from the target. There are two common forms. The first involves malicious code; this code is usually hidden within a file attached to an email. The intention is that an unsuspecting user will click/open the file; for example, 'I Love You' virus, 'Anna Kournikova' worm.

9. A phishing technique that has received substantial publicity of late is “vishing,” or voice phishing. Vishing can work in two different ways. In one version of the scam, the consumer receives an e-mail designed in the same way as a phishing e-mail, usually indicating that there is a problem with the account. Instead of providing a fraudulent link to click on, the e-mail provides a customer service number that the client must call and is then prompted to “log in” using account numbers and passwords.

The other version of the scam is to call consumers directly and tell them that they must call the fraudulent customer service number immediately in order to protect their account. Vishing criminals may also even establish a false sense of security in the consumer by “confirming” personal information that they have on file, such as a full name, address or credit card number [4].
Vishing actually emulates a typical bank protocol in which banks encourage clients to call and authentic ate information [5]

III. CASE STUDY EASE OF USE

As Social Engineering is the most powerful attack, we tried to check how effective the social engineering on the Linux. Linux is considered as most secure operating system but as we have discussed even the most secure system can be break by targeting weak link (people). Following case study shows the impact of social engineering if plugged with Spyware.

3.1. Implementation of Case Study

We have created a Spyware for the Linux which logs the information typed by the user in Linux environment. We have not put the Spyware on the wild means in real environment but to get statistics related to Spyware with social engineering tactics, we tried to achieve it three ways and all these techniques are based on social engineering [6].

Case-1: Enthusiasm of fun: As for this attack, first we gather information like we used the person whom we know. We gathered the information like he uses the Operating system as Linux; He is fond of Linux shell script programming. Second stage is relationship development which is already established as we choose person who trust us. We sent it to friend who uses Linux as desktop operating system in mail. Subject line of the mail was “Shell Script for Fun”. As frequently you got mail from your friend having attachment, you open it as it pretend to be from friend and safe. You get trapped because even you can send mail with any fake name using open mail relay SMTP servers. This is psychological strategy and it is customized attack, as we have chosen the individual. Some parasite writers use customize approach for

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 5, May 2019

some specific victim while some uses general approach to trap unknown victims and if that technique get successful then many people will get trap in it.

Case-2: Eagerness to know great thing: Second case we gone for same principal first information gathering, relation establishment and then deception. We choose persons who are fond of hacking and cracking activity. Case-2 targets such user who loves hacking and cracking. Even on internet, if you search for free tools for hacking and cracking, you will get it for free. But many of such software itself hack your system. On internet: I have put link of this shell script with Name "Tool to hack in Windows" to friend. And they clicked on it, downloaded it and ran it.

Case-3: Hoaxing: As people think, Linux is secure than windows but don't know by what percentage and they want information on this aspect. So fake Linux report containing the Shell Script as the case. As a news to friend – Linux sec urity report. As people normally follows the link as it is report on Linux. As all this techniques uses social engineering, human get trapped. Our spyware requires the root privileged.

3.2. Other Example of Social Engineering Attacks

Social Engineering is used by hackers and crackers to hack the target machine or to spread virus and Malware application. To introduce the Social Engineering, we have to give some real example, which can be understood easily by the non-technical person.

Following are the few attacks for spreading Spyware

1. Piggybacked software installation: User is lured to install the software for free and with that software automatically some Spyware get installed which will monitor and even tamper your data. That software might be claiming of game or media player or any useful software [1].
2. Mail: you get mail from your friend or from unknown mail id with some interesting or alert subject line like "Hey check your machine" or "You might be infected" you open it and you get infected .
3. Fake anti Spyware: There are various utilities claiming anti-Spyware but actually they are Spyware or some application enticed with hacking tool but actually hacking your system. The weakest security link, which concerns playing with human psychology to get the confidential details out of him by appearing to be 'genuine and concerned'
4. Spam mail claiming "You won the lottery" or claiming to be selling some genuine medicine for good result. This all are the social engineering to lure the target to provide some information which can be used to gain financial or social or personal gain.

IV. PREVENTION

User education is the first and most powerful defense against social engineering, backed up by strong, clear (written) policies that define when and to whom (if ever) users are permitted to give their passwords, open up the server room, etc. Strict procedures should be laid down. By implementing authentication system (smart cards/tokens or, even better, biometrics), you can thwart a high percentage of social engineering attempts. Even if the social engineer manages to learn the password, it will be useless without the second authentication factor. A successful defense against the social engineering depends on having good policies in place ensuring that all employees follow them Social engineering attacks are most powerful attacks as the defense against it is not the software system but the people which in themselves quite unpredictable. Still using few counter measures we can prevent some of the attacks.

Following are the prevention techniques for personal defense

1. We have to be suspicious of any e-mail with urgent requests for personal financial information or threats of termination of online accounts.
2. Unless the e-mail is digitally signed, you can't be sure it wasn't forged or "spoofed." because any one can mail it by any name hence when it is stating some important better to check for the full headers.
3. Phishers typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc. and such information normally won't be asked by the genuine organization online.
4. Phisher e-mails are typically not personalized, while valid messages from your bank or e-commerce company generally are. "Phisher e-mails start some thing like "Dear customer" but there are some attacks which are customized or more advance which uses your personal information and if the attack is specifically for you then it will be customize like our case sudy.
5. When contacting your financial institution, use only channels that you know from independent sources. (e.g., information on your bank card, hard-copy correspondence, or monthly account statement), and don't rely on links contained in e-mails, even if the sites looks genuine.

6. Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser. Check in the address bar URL must start with https:// instead of http://
7. Regularly log into your online accounts and change password frequently.
8. Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.
9. Don't assume that you can correctly identify a website as legitimate just by looking at its general appearance.
10. Avoid filling out forms in e-mail messages or pop-up windows that ask for personal financial information because it might be used by spammers as well as phisher for future attack.

Following are the few counter measures for the organizational institute.

1. Well defined and documented security policy: In this process company set the standards and guidelines form the foundation of a good security [7].
2. Acceptable usage Policy: for acceptable business usage of email, computer system, telephone and network as well as other hardware like pen-drive.
3. Personnel security: A screening of prospective employees, contractor to ensure that they do not pose a security threat to the organization [3].
4. Information Access Control: Password usage and guidelines for generating password, access authorization and accounting procedure, installation procedure. Automated password reset and synchronization tools can lift the responsibility of managing password from tech support and help desk without placing an undo burden on end user [3].
5. Protection from Malware like Spyware, virus, adware, Trojan etc using software systems. Like firewalls, antispyware and anti-virus software with regular updating of patches. These will ensure filtering of major security breach incidents [3].
6. Awareness and Education: Giving education to the user about the common techniques employed and used by the social engineer is an important part of security system. For example, a knowledgeable user can be advised that he/she should never give out any information without the appropriate authorization and that he/she should report any suspicious behavior 9][10]
7. Audits and compliance: Policy gets effective only when it gets implemented and everyone conforms to the policy. Hence auditing the usage and make sure everyone compliance to the rules [9]
8. Security Incident Management: When a social engineering attacks occurs make sure service desk staff knows how to manage such attack. As each attack is different, system will get new data and hence its need to be manages for future use. Hence reporting and storage of such incident should be done properly

v. CONCLUSION

We might have the most secure network or clear policies still as humans are unpredicted due curiosity and greed without concern for the consequences, we could face our own version of a Trojan tragedy . A paradox of social engineering attacks is that people are not only the biggest problem and security risk, but also the best tool to defend against these attacks. Organizations must fight social engineering attacks by establishing policies and procedures that define roles and responsibilities for all users and not just security personnel. As well as organization must ensure that, these policies and procedure are executed by users properly hence regular training needs to be given on the latest such incidents.

REFERENCES

[1]. DataLossDB, “Data Loss Statistics”, Oct. 2009: http://datalossdb.org/statistics
[2]. A Karakasiliotis, M Papadaki and SM Furnell, Assessing End-User Awareness of Social Engineering and Phishing, Proceedings of the 7th Australian Information Warfare and Security Conference, 2006.
[3]. Mahmoud Khonji, Youssef Iraqi, Andrew Jones, Phishing Detection: A Literature Survey, IEEE Communications Surveys & Tutorials, 2013, 15(4), 2091-2121.
[4]. Joseph A Cazier and Christopher M Botelho, Social Engineering’s Threat to Public Privacy, Proceedings of the 6th Annual Security Conference, Las Vegas, NV, 2007.
[5]. Anubhav Chitrey, Dharmendra Singh and Vrijendra Singh, A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model, International Journal of Information and Network Security, 2012, 1(2), 45 – 53.
[6]. Thomas R Peltier, Social Engineering: Concepts and Solutions, Information Systems Security, 2006.
[7]. Devin Luco, The Art of Social Engineering: A Research Note, http://anniesearle.com/ 2015.
[8]. Megha Gupta and Sameer Agarwal, A Survey on Social Engineering and the Art of Deception, International Journal of Information and Education Technology, 2012, 1 (1), 31 – 35.
[9]. Joseph A Cazier and Christopher M Botelho, Social Engineering’s Threat to Public Privacy, Proceedings of the 6th Annual Security Conference, Las Vegas, NV, 2007.
[10]. L J Janczewski and Lingyan (Rene) Fu, Social Engineering Based Attacks: Model and New Zealand Perspective,Proceedings of the International Multiconference on Computer Science and Information Technology, 2010.
[11]. R Chandramouli, Emerging Social Media Threats: Technology and Policy Perspectives, Cyber Security Summit,2011.
[12]. Ugiomo Odaro and Benjamin Sanders, Social Engineering: Phishing for a Solution, A Research Note http://www.kaspersky.co.in/ 2015.