International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Evaluation of Human Behavior Weaknesses in Social Engineering

Said Masihullah Hashimi[1], Komal[2]

[1]Student, Amity University, Amity Institute of Information Technology, Gurgaon, Haryana, India

[2]Assistant Professor, Amity University, Department of Computer Science and Engineering, Gurgaon, Haryana, India

Abstract: ***Security breach and hacking techniques has been available in numerous ways in this rapidly developing era of technology in order to gain access to desired information. The human approach of this phenomenon is often termed as 'Social Engineering' and it is probably the most difficult one to be dealt with. This paper describes Social Engineering non-technical approaches used to exploit human behavior and will point out or those behavior weaknesses that can be compromised and taken advantage of it to pull out a scam or breach a network security.***

Keywords: Social Engineering, Impersonation, Eavesdropping, Piggybacking, Dumpster diving

1. Introduction

Social Engineering refers to psychological manipulation of people into performing actions or reveling and disclosing confidential information that an attacker can used to do any other sort of attack. This is a type of confidence trick for the purpose of information gathering, system access or committing a fraud [1]. Human behavior also has many vulnerability areas and as part of social engineering, hackers never hesitate exploiting that vulnerability, in other words it can be psychological manipulation of people of convincing them to reveal confidential information.

2. Social Engineering Phases

Social Engineering has steps and phases to follow by any attacker and it may differ from person to person.

2.1 Basic researching on the target (a company or a person) by doing dumpster diving, website surfing and getting the employee details from any different sources.

2.2 Find a victim (an employee) who is frustrated and who can do any activity that can make a loss to the company.

2.3 Developing relationship with that person (employee) and give him the confidence to cooperate.

2.4 Exploiting the relationship of that person and makes use of it in the last phase.

3. Social Engineering Techniques:

There are two types of social engineering, technical and non-technical (Human Social Engineering). In this paper, we will be talking and discussing about non-technical or human social engineering approach only [2].

Figure 1: Social Engineering Phases

3.1 Human Social Engineering

3.1.1Impersonation

The impersonation is an act of pretending to be a legitimate person for the purpose of entertainment or fraud. This is the most common social engineering technique where attackers pretend to be someone authorized to get access to confidential information. Attacker may impersonate as an authorized person either by personally or by any communication medium such as email or phone call. Impersonation helps attacker in the tricking target to reveal confidential information.

3.1.2Eavesdropping

Eavesdropping is the process of secretly listening to the private conversion of others without their consent. As an example, unauthorized listening or intercepting of the calls, messages, emails or faxes of others and misusing them.

3.1.3Shoulder surging

Shoulder surfing is the process of spying of an electronic device user in order to obtain their personnel identification number (PIN) or password.

3.1.4 Dumpster diving

Dumpster diving is a popular human based social engineering technique where an attacker try to find any valuable information in some one's trash, like contact information, their bank account statement or any such thing that can be used to do identity theft.

3.1.5 Tailgating or Piggybacking

Tailgating is a scenario where an authorized person wearing a fake ID or not restricted to a restricted area that follow an authorized person and try to enter the secure area through that door. And piggybacking can be a scenario where the attacker may make excuse of forgetting ID or access card and may ask to enter without proper identification card, this can be an example of Piggybacking social engineering.

3.1.6 Reverse Social Engineering

In reverse social engineering an attacker may damage your

system and equipment first, and then they will contact you and try to impose as IT support guy to solve your problem. In the mean time they may install malware in your system to monitor you or track your activities, get your confidential information and share to those who demand for it.

4. Human behaviors that affects more in being exploited in Social Engineering

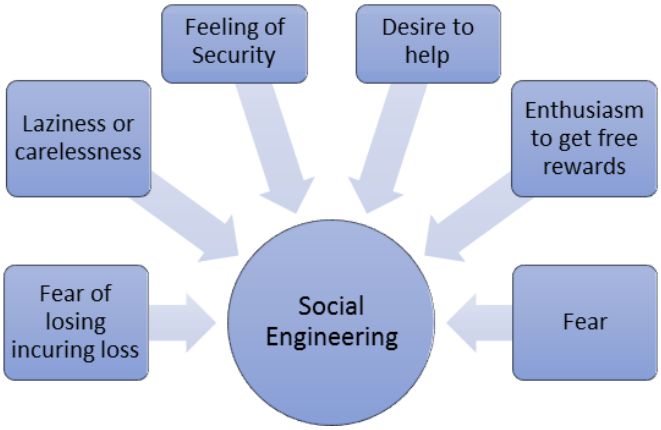

Figure 2: Human Behaviors that Affects more in Social Engineering

There are a lot of human behaviors that can be exploit in certain situations by an attacker in social engineering context, here we will be going to discuss and touch on some of them.

4.1 Fear of incurring Loss

This behavior is concerned about a loss over a period of time, like not paying something on time and it can be exploit by impersonation where a person may contact the victim and act as authorized individual to get the desired information from the victim [3].

4.2 Laziness or carelessness

The carelessness of humans can be exploited because humans often feel apathetic towards setting up proper defense mechanisms. Examples of attacks against our carelessness are dumpster diving which involves the collection of the trash from a particular target and sorting it for useful information such as thrown documents with signatures which are left there without being shredded.

4.3 Feeling of security in a comfort zone.

The next human quality that social engineers exploit is the feeling of security in a person's comfort zone, which in most cases includes the work environment. Humans feel secure at their workplace, to a greater or lesser extent, and they are more likely to be less perceptive of possible threats, scams and dangers that exploit this sense of security. Their guard will be down when a social engineer tries to take advantage of their work environment.

A common abuse of a person's comfort zone is impersonating an insider. The most common impersonation is of the IT staff, as people in the company generally have less knowledge of how the IT systems are maintained and they are in a way ignorant in this area. Social engineers can also pretend to be janitors, repairmen, even firemen.

4.4 Desire to help

Attackers will mostly use the methods of piggybacking followed by dumpster diving. Leaving the door open in a smoking area or another section of office like cleaning and maintenance service area may cause such incidents where an intruder with fake ID can enter and pretend to be one of the staff and help an employee regarding something, as we discussed the example of IT guy in pervious method who can be dressed up as IT team and ask to help you fix a security issue in your system or do a routine checkup.

4.5 Enthusiasm to get free rewards.

Often some employees use ways and methods in order to impress their bosses and to get free reward, these methods may not be according to company policy such using third party computer applications or downloading a file format of a report which could be malicious and used as bait by some intruder. This behavior can lead to information theft, security breach and many other malicious activities.

4.6 Fear

Fear can be exploited by providing a short time frame to do a certain job in which the victim has to perform something, by relying on authority, an example can be impersonating a CEO or some important manager in the company or by forcing and placing the victim into an uncomfortable position to do something.

5. Suggestions on prevention Human Social Engineering attacks

After deep assessment of the mechanisms and tactics that attackers use in Human Social Engineering. This paper comes to findings and suggestions in order to ensure security and prevent these kinds of attacks. Following are some points to consider in order to maintain security in any organizational working environment [4]. We need to have a clear security policy that should cover all the relevant points where information exploitation is felt, the main points are mentioned as follows:

5.1 Well Documented Policy

5.1.1 Personnel security

Properly checking and screening employees and contractors to ensure that they do not poise a security threat to a firm or organization when they are hired.

5.1.2 Information Access Control Policies

Access authorization, Password generation, Remote access policies and other important points should be taken in consideration.

5.1.3 Scheduled Monitoring

Regular monitoring to ensure that the policies are properly applied and being taken serious by employees to ensure security.

5.2 Risk Assessments

Assessing risks in a systematic approach to help in managing and understanding the factors that causes risk in an organization and can adversely affect the overall system [5].

5.3 Awareness and Education

Educating employees about the risks of social engineering by conducting workshops and trainings and making them aware regarding the techniques that intruders use to gain access to their desired means.

5.4 Identity Management

Using proper employee identification procedure and the access policies to different sections for them according to their positions and rights

5.5 Operating Procedures

Clear procedure for processing operations in an organization and maintaining workflow among employees.

5.6 Security Incident Management.

Recording the incidents such as security breach, information theft etc. along with the victim information, reasons of attack and weakness points in order to track it and fix the problem to prevent such incidents in the future [6].

6. Conclusion

Human Social Engineering attacks cost a lot every year and damages organizations due to smallest mistake and carelessness of an individual in an organization. A number of vendors and companies are using some tools to prevent such attacks, which is costly as well as not much efficient. A logical way to stop such attacks is to educate employees, provide them trainings and teach them on how to deal with emotions and behavior that is vulnerable of being exploited. And lastly consider the points that this paper suggests on how to prevent human social engineering attacks.

References

[1] Sarah Granger, “Social Engineering Fundamentals Part 1: Hackers Tactics”, March 2006.
[2] Arthurs Wendy, “A proactive Defense to Social Engineering”. SANS institute, Aug 2001.
[3] Ian S. Kaufer, “Human Exploits in Cybersecurity: A social Engineering Study”, *December 2016*
[4] Bernard Oosterloo, “Managing Social Engineering Risks”, October 2008.
[5] Dimensional Research, “The Risk of Social Engineering on Information Security: A Survey of IT Professionals”, www.greycastlesecuryt .com, September 2011.
[6] Luo X, Seazzu A, “Social Engineering: The Neglected Human Factors for Information Security Management”, Information Resources Management Journal, Volume 24, Issue 3, pp. 1-8.