NOVATEUR PUBLICATIONS
JournalNX- A Multidisciplinary Peer Reviewed Journal
ISSN No: 2581 - 4230
VOLUME 7, ISSUE 4, Apr. -2021

SOCIAL ENGINEERING TECHNIQUES AND MITIGATION MECHANISM

Joseph Paulman
Modul University Vienna- Austria

Frederick Je
Hamburg College- Germany

ABSTRACT:

Cybersecurity is an integral part of the computer systems especially in current time where data is a very valuable asset a company or an individual can have. Cyberattackers are increasing in number and the attacks have increased both in terms in advancement and quantity. Without proper protection the individual or the company is at the risk of losing the data by the cyberattackers. Social engineering techniques are the type of cyber-attacks that does not focus on the vulnerabilities of technology but they are targeted at the susceptibility of human emotions. Social Engineering techniques depends on the gaining human trust. Genrally, the weakest link in security systems are not the technology but the human element. I have choosen this field of research because I myself have been a target of numerous cyber-attacks and I wish to educate myself to protect myself from the social engineering attacks in the future and also want to develop certain methods which enable individuals or companies to protect themselves from the attacks based on social engineering techniques.

Keywords: Cyber Attacks, Social Engineering Techniques, malwares, victim, attacker.

INTRODUCTION:

Social engineering techniques are based on the vulnerabilities of the human emotion. They work when the gain of trust of victims by the cyber attackers. The normal cyber-attacks are based on attacking the vulnerabilities in technology whereas in the social engineering techniques the attackers may disguise himself by false indentity and trick the victim to reveal sensitive and confidential information. Social engineering techniques depends on the natural human tendencies and emotional reaction in emergency situations or where its necessary to act quick without thinking based on our emotional reactions. The attackers intentionally create such situations where victims are given no option to think but to act. Social engineering depends on the psychological manipulation, for achieving this purpose the cyber attacker gathers background information of the intended victim to formulate a attack. So, its very important not to reveal your personal information online anywhere at all costs. Attacks based on social engineering techniques are easier and have high success rates than the ttacks based on technology because its easier to trick the victims than the rigid technology. It's for this reason, we can say that the weakest link in the security system is not the technology but the

1 Social Engineering techniques:

1.1 Phishing:

Phishing is a type of social engineering attack in which the victim receives a email from the attacker disguised himself as trusted person requesting sensitive information which is then used by the attacker for his own

personal gain. In phishing, the attacker disguises himself as a trusted entity ,for example a manager from the company or employee of his personal bank. The attacker then creates a urgent situation or circumstances in the mail where the victim has not enough timeto think and act based on emotional reaction. Its not always the case of urgency sometimes the attacker sends a attachment in the email disguising himself as a employee from a company to download an attachment which contains malware.

1.2 Spear Phishing:

Spear phishing is different from normal phishing in that the attacks are targeted towards a well researched individual. In normal phishing the attacks are directed towards a large group of people with low success rates. While in case of spear phishing , the attacker researches the traits, background and characteristics of the victim and tailor the mail so that the victim proceeds with the plan the attacker has intended. Spear phishing has high rates of success than normal phishing as the attacks are formulated specifiaclly towards a person. For example , an attacker may research a individual in the company who is found to be loyal to the CEO and the company, always obeys the CEO and is quick worker, the attacker may disguise himself as CEO and mail the targeted employee that he requires to transfer funds immediately to a company which is a urgent thing to do and CEO himself cannot do it because he was travelling. The employee may proceed with the transfer as he prone to be loyal.

1.3 Baiting:

Baiting is dependedent on human emotions of greed and curiosity. Baiting attack is done by attracting the victim for a prize or promotion by sending a infected file as mail. For example, the attacker may mail all the employees of the company an attachment saying that it is a free promotion for their extraordinary service to the company, the employee may open the attachment and be infected by the file. Attackers may also take advanatge of cuurent situations in the world to formulate the attack. For example the attacker may take advantage of the coronavirus condition in the world and may mail individuals disguising himself as the employee of the government ,may request the victim to enter the credit card details so that he/she may receive a relief fund from the government. The gullible victims may enter the details.

1.4 Pretexting:

Pretexting is another form of social engineering attack where the attacker disguises himself anauthority from the police agency, banking, tax officers, investment investigators or any other form of authoritative figure. The attacker then makes a good pretext with the victim saying that he needs to verify the details of the victim before providing further details. The victims may believe the good pretext and assume the attacker as a real authoritative figure. The victim may receive the a call from the attacker after the good pretext he may say that a employee from the bank may arrive at home to receive the cash for the loan. In any event it is best to protect yourself from the pretext.

1.5 Tailgating:

Tailgating relies on the physical access of the computer systems. The attacker may gain the trust of the employee of the company by saying that he is a sales person, he may then enter the company which may give the attacker the access to the computers which he may further exploit.

3.0 MITIGATION MECHANISMS:

3.1 Human based mitigation:

Human based detectiion involves human intervention in detecting and preventing social engineering. Human based mitigation depends on the judgement of the humans. Humans can be better trained to become aware of the social engineering techniques and identify when they are being targeted by them.

3.2 Policy and auditing:

The company may develop certain policies in detecting and preventing social engineering from taking place. Many companies extensively use the policies for preventing social engineering attacks. Auditing is about testing the employees for the level of awareness of social engineering techniques among the employees. Both auditing and Policy making form a crucial part in preventing social engineering attacks from happening.

3.3 Education, training and awareness:

Education , training and awareness is one of the approach the company takes in preventing the social engineering attacks from happening. ETS is especially valuable for newly employed staff. The company must give proper orientation to the employees about the ETS in social engineering attacks. Further , the companies can develop an interactive and game-based ETS portals to educate the employees about the Social Engineering attacks.

4.0 CHALLENGES IN HUMAN BASED MITIGATION:

There are some challenges in the human based mitigation which can only be overcome with technology based m mitigation. Even after the extensive education, training and awareness in the social engineering attacks , it finally depends on the decision of humans in the attack situations. Even after training, attackers can still psychologically manipulate the victims or manipulate their emotions to gain advantage. Another problem is the attackers targets the newly employed staff as they are the weakest link in the organization who can be easily targeted.

5.0 TECHNOLOGY BASED MITIGATION:

There are many ways to protect from the social engineering attacks using technology. Some of them are discussed below.

5.1 Sensors:

Physical tokens have been used as trusted identity verification methods in most of the areas. The chip in the token is scanned for verification and if they are genuine .

5.2 Biometrics:

Social engineers may attempt to impersonate the profile of a employee by creating a profile of their character . Biometrics does not rely on the perceived identity but on the biological traits of the employee so its difficult to impossible to mimic the biological traits.

5.3 Honeypot:

Honeypot is a system that is created to imitate an existing working system to tap the attackers and learning their behaviours.

6.0 ISSUES WITH TECHNOLOGY BASED MITIGATION:

The additional use of the technology cost the organization more to maintain the technology and to run it. Management of these technology requires additional employees which is further added to the cost to the company. There is a chance that the technology can malfunction which brings

huge damage to the business. This may be in the form of software flaws or design defects.

7.0 SUMMARY:

Social engineering takes advantage of the human emotions and the psychology. It involves the research of the victim, trust building, searching for vulnerabilities and attacking. It has been a threat for a longtime for both the individuals and the companies alike. There is still no complete solution to eliminate the social engineered attacks. Education, training and awareness can form the human element of the mitigation but it has its drawbacks. Technology based mitigation may tighten the security but it also has its own drawbacks and they cost more to maintain and function. The threat of social engineering cannot be eliminated completely, the best thing that can be done to prevent social engineering attacks is to continue researching how the individuals and organizations are exploited leading to the improvements of the security standards.

REFERENCES:

1) https://www.mdpi.com/1999-5903/ 11/ 4/89/pdf
2) https://www.sciencedirect.com/science/article/pii/S0957417413001255
3) http://ra.ethz.ch/CDstore/www2010/www/p1139.pdf
4) https://www.researchgate.net/publication/256841808_Phishing_Detection_A_Literature_Survey
5) https://hbr.org/2003/04/are-you-the-weak -link
6) https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/
7) R Alugubelli. (2016). Exploratory Study of Artificial Intelligence in Healthcare. International Journal of Innovations in Engineering Research and Technology, 3(1), 1–10. Retrieved from https://repo.ijiert.org/index.php/ijiert/article/view/2699