International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

Social Engineering Measurements and Analysis

Dr. Abdulrazaq Alsuhail Almutairi, Information & Computer Center
The Public Authority for Applied Education and Training, The Ministry of Education
State of Kuwait
AZ.ALSUHAIL@PAAET.EDU.KW

Abstract

Social engineering has become one of the most widely used techniques in overcoming security mechanisms. It is an attack targeting the human element involved in a security system. In such types of attacks, the assailant manipulates legitimate users of the system, using a host of physical and psychological compromising methods. Thus, a compromise of the underlying infrastructure may occur for possible exploitation. It remains a popular method of bypassing security because attacks focus on the weakest point in the security mechanism, the staff of the organization, rather than directly targeting electronic and cryptographic security algorithms. In this paper, a framework is proposed to analyze and measure social engineering threats in an organization. The results obtained by the analysis and measurements will then lead to having a security policy and control, thereby reducing the chance of social engineering attacks occurring.

Keywords

Computer Security; Social Engineering, Phishing, Vishing

1. Introduction

Social engineering is an act that convinces a person to take an action, which may or may not have a negative impact. In the computer security context, social engineering is considered as a non-technical type of intrusion that mainly depends on human responses and normally involves deceiving people into cracking normal security procedures. Social engineers exploit situations where there is no awareness of the value of the information users possess. Hasle [1] provides a concise definition for social engineering as follows:

"Social engineering is using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker. It could be something as simple as talking over the telephone to something as complex as getting a target to visit a Web site, which exploits a technical flaw and allows the hacker to take over the computer."

Goodchild [2] noted a survey carried out with 850 IT and security experts based in the U.S., Canada, U.K., Germany, Australia and New Zealand. 48 % of those experts reported that they had been victims of social engineering and had experienced 25 or more attacks in the past two years. The survey also states that social engineering attacks cause financial losses of between $25,000 - $100,000 per security incident. According to the FBI [3], business email compromise (BEC) scams have resulted in losses of £2.4 billion ($3.1 billion) as of May 2016.

Another survey [4] conducted by AGARI in 2016 found that 60% of surveyed security experts reported their organisations were, or may have been, the target of at least one social engineering attack in the past year. The survey also reveals that 65% of those who were attacked had their employees' credentials compromised because of the attacks. They also added that 17% of those attacks caused financial accounts to be breached. Dr Markus Jakobsson, chief scientist for AGARI, [4] elaborated on the impact of social engineering attacks as follows:

"Email-based attacks using social engineering are enabling cyber-criminals to steal corporate secrets, carry out politically motivated attacks and steal massive amounts of money. We expect to see a catastrophic growth of these types of attacks in the future, fuelled by both their profitability and the poor extent to which businesses are protecting themselves, unless these organisations begin taking the necessary technology-based countermeasures to prevent these attacks."

In this paper, a framework is presented to help organizations analyse and measure social engineering threats. The second section in this paper presents a brief background, including going through different stages of a social engineering attack, and different types of attacks. The third section presents the proposed approach. The fourth section walks through some of the related works, an explanation for the proposed methodology and how to apply it. The final section presents the conclusion and suggested future work.

2. Background

A. Social Engineering attack phases

There are different types of social engineering attacks. Most of such attacks go through the same phases, presented in figure 1 below.

- The first phase is to gather information. This includes information from different sources such as phone books, web sites etc. Information can also be obtained from previous social engineering attacks. The gathered information will be then employed to build a relationship with the target.
- The second phase is to build a relationship with the target by using the natural human tendency. The goal of this phase is to establish trust with the victims [5].

ISSN:2319-7900

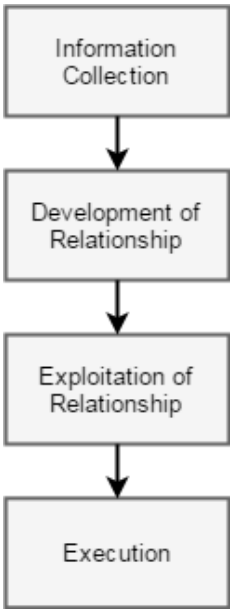

Figure 1: Social Engineering Phases

- The third step is to exploit the trust established in the previous step by getting the target to uncover sensitive information, such as credit card details, login credential etc.

- The fourth step is the execution where the attacker attempts to achieve the end goal; for example, accessing confidential data, deleting files, or changing permissions.

B. Examples of social Enginnering attaccks

B.1 Phising

Phishing scams are the most widely used types of social engineering attacks employed these days. Such types of scams use both social engineering and technical subterfuge to obtain personal identities and financial account credentials. Social engineering schemes utilize e-mails to forward users to forged websites, implemented to deceive recipients into providing sensitive information, such as credit card details, account login, passwords and other personal information. Phishers normally convince their victims to respond by appropriating brand names of banks, e-retailers and credit card companies. Technical subterfuge schemes inject software into the victims' machines to get credentials directly, often using Trojan key logger spyware [6].

Deceptive phishing is one of the most common types of phishing scams. In such types of phishing, attackers impersonate a legitimate organization and attempt to steal people's personal information or login credentials. Spear phishing is an example of phishing scams, where attackers customize emails with the victims' name, role, company, and telephone number. This sort of customization aims to trick the recipient into trusting the sender.

B.2 Baiting attacks

Baiting is one of the social engineering attacks based on human's curiosity. A typical example of such attacks is a scenario where attackers employ a malicious file presented as a software upgrade. Once the malware is installed on the victim's machine, attackers will compromise the machine, gaining full access [7].

B.3 Quid Pro Quo attacks

A Quid Pro Quo attack represents a social engineering attack, where fraudsters promise a service based on the execution of a specific action in exchange for information or access. The most common quid pro quo attack occurs when a hacker pretends to be an IT professional for a large organization. That hacker approaches their victims via phone then offers them a service, such as an upgrade or software installation. They then request victims to switch off the Anti-Virus application temporarily to inject the malicious application [7].

B.4 Pretexting

Pretexting attacks refer to the practice of presenting oneself as someone else to get private information. Normally, fraudsters create fake identities and use these to build a trust with victims [8].

3. The Proposed Approach

A. Overview

In the social engineering context, it is the human element that represents a security hole. Measuring the threat level of social engineering attacks involves finding out how easy they can be dragged to achieve the attacker's aim. In other words, it is necessary to measure the awareness of social engineering among the employees of an organization. Measuring that level of awareness will shed the light in placing security policies and controls.

The proposed approach in this paper evaluates the threat level of social engineering in an organization by simulating social engineering attacks, then collecting data about the behaviour of employees towards those social engineering simulated scenarios. Fig. 1 shows the work flow in the proposed approach

B. Set Social Engineering Scenarios

In the first phase, a number of social engineering scenarios need to be designed. The scenarios need to consider all communication tools that employees use in their daily business activities, such as email, phones, and online chat. For each scenario, all possible behaviours need to be listed. A numerical value will then be assigned to each possible behaviour. Some of those numerical values will be used later to generate statistics that will help in making decisions related to setting security settings and policies.

ISSN:2319-7900

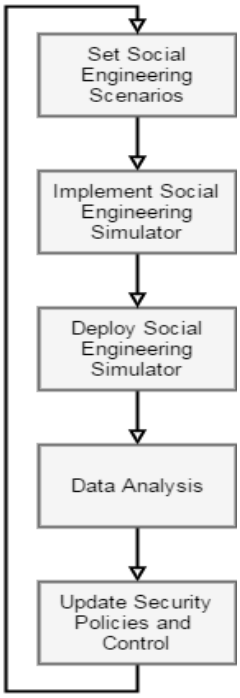

Figure 2: Relation between different models

C. Social Engineering Simulator

The simulator in this context is responsible for carrying out scenarios designed in the previous step. In addition, it translates human behaviour towards those scenarios into numerical values. The simulator is connected to a data-base that holds information about the social engineering scenarios to be performed, all possible behaviours towards those scenarios, and the behaviour of each person exposed to those scenarios. Fig. 3 shows the simulator's entity relationship diagram.

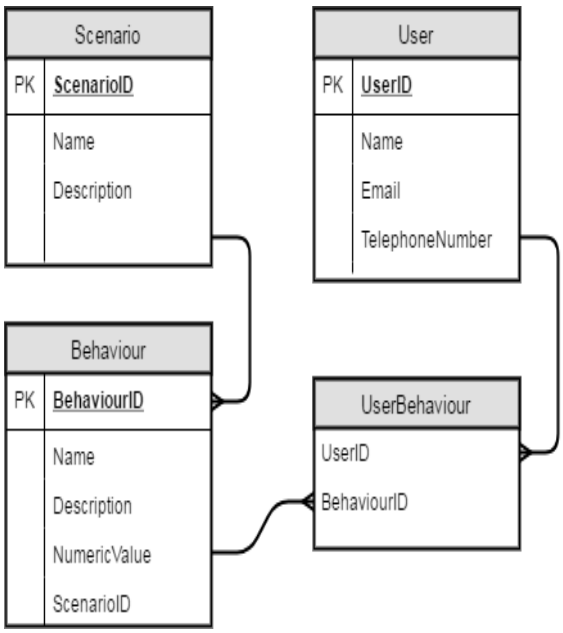

Figure 3: Relation between different models

D. Deployment

At this stage, the simulator is run by the system administrators. The simulator runs all set scenarios in the data-base and collects information based on user behaviour.

E. Data Analysis

Results and data collected after running the simulator are analysed to find out areas that need some actions to improve level of security.

F. Update Security

Based on the statistics generated, security policies and rules are reviewed and updated to reduce the risk of social engineering attacks.

4. Experiment

A. Overview

The proposed approach was applied to a group of 10 people with a marketing and sales background, working in a company providing insurance services. In this experiment, three scenarios were implemented. The first one involved communication through emails, the second one involved interaction with messages prompted on victims' machines, and the third one involved communication through phones. In each scenario, three people were involved. Participants involved in this experiment were not aware of any details about social engineering scenarios to be carried out.

B. Scenarios

1. Spear phishing:

In this scenario, an email was sent to all participants, each email included the person's name while the content included a link to a spread sheet file containing many contacts. The sender's email address looked as if it came from a genuine organization. There were two possible behaviours for such a scenario: responding to that mail by clicking on the link; or ignoring the email. The simulator updates the database with the first behaviour once the link is clicked, while the second behaviour is recorded, if no response is obtained within 2 business days.

2.* Baiting attacks*:

In this scenario, participants' machines have been configured with a script that loads their web browser with a page prompting a message saying that the system needs to be upgraded to improve security. The message will give an option to proceed or ignore.

3.* Quid Pro *Quo* attacks*:

In this scenario, participants were contacted over the phone. The caller pretended that he was an IT support engineer offering to fix some issues related to the network. The caller asked the participant to provide their credentials in order to fix the issue. There were two possible behaviours in such a scenario. The first one is where a participant provides all the details without trying to confirm the identity of the caller. The second category represents participants, who decide not to proceed with

ISSN:2319-7900

the call after being asked to provide their login credential.

C. Results

Fig.4 shows the results obtained after implementing and deploying the three scenarios. The results show that most of the participants (90%) responded to the first scenario by opening the link included in the email sent. In the second scenario, 60% responded to the prompt message by proceeding with a suggested upgrade. In the third scenario, none of the participants proceeded with the call. The results indicate that some security policies and control need to be around access to emails and websites. In addition, the participants need to be trained to be aware of security around emails and websites.

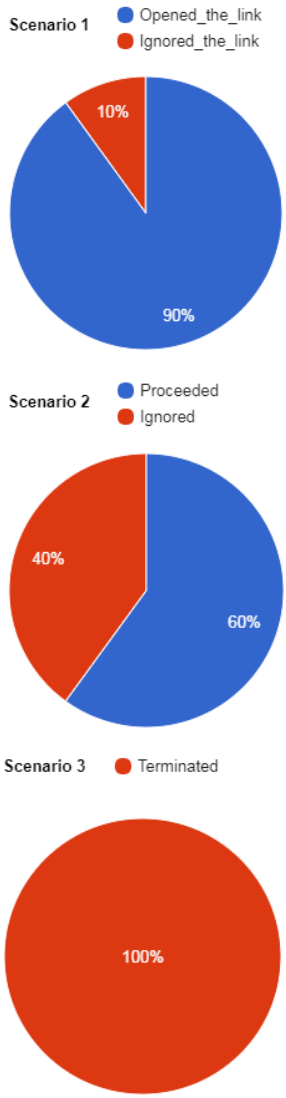

Figure 4: Results obtained in the experiment

5. Related Work

Mataracioglu and Dingli [9] conducted an analysis of the social engineering tests that were carried out in several Turkish public agencies. The analysis showed that the employees in those agencies have a lack of information security awareness and can be easily deceived into leaking sensitive information.

Hasle et al. [10] proposed a social engineering resistance metric. The research also involved implementing software to obtain metric test data. The research also included carrying out an experiment involving 120 participants. The results of the experiments have shown how social engineering represents a weakness point in a security system.

6. Conclusion and Future Work

This paper has provided an approach that facilitates measuring and analysing the impact of social engineering attacks in an organization. The approach was applied among ten participants by exposing them to three social engineering attack scenarios, each of those scenarios representing a different social engineering attack. The results suggest some changes in security policy and control around email and websites access areas.

Future work will include more scenarios that cover as many social engineering scenarios as possible. In addition, the deployment stage will be improved in a way that all scenarios will be automatically driven without any human interventions.

7. References

[1] M. Nohlberg and S. Kowalski, “The Cycle of Deception - A Model of Social Engineering Attacks”, Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008).

[2] J. Goodchild, “Social engineering attacks costly for business”, [Online] Available from: http://www.csoonline.com/ [Accessed: 20th April 2017]

[3] SecurityWeek News, ”Losses From Business Email Compromise Scams Top $3.1 Billion: FBI”, [Online] Available from: https://www.agari.com/news-and-press-releases/ [Accessed: 19th May 2017]

[4] AGARI, “New Agari Study Reveals 60 Percent of Enterprises were Victims of Social Engineering Attacks in 2016”, [Online] Available from: http://www.csoonline.com/ [Accessed: 20th April 2017]

[5] M. Nohlberg,, “Social Engineering: Understanding, Measuring and Protecting Against Attacks”, University of Skövde, 2007.

[6] J. Hong, "The Current State of Phishing Attacks", Communications of the ACM, 2012, vol.55, no.1, p.p 74-81.

[7] M. Alexandar, “Methods for Understanding and Reducing Social Engineering Attacks”. SANS Institute Infosec Reading Room, 2016 [Online] Available from: https://www.sans.org/reading-room/whitepapers/critical/ [Accessed: 3rd june 2017]

ISSN:2319-7900

[8] M. Spinapolice, "Mitigating the risk of social engineering attacks", Rochester Institute of Technology, 2011.

[9] T. Mataracioglu and S. Ozkan, "User Awareness Measurement Through Social Engineering", National Research Institute of Electronics and Cryptology, 2011.

[10] H. Hasle, Y. Kristiansen, K. Kintel, and E. Snekkenes, "Measuring Resistance to Social Engineering", Proceedings of the First international conference on Information Security Practice and Experience, 2005, p.p 132-143.