INFORMATION SECURITY

SOCIAL ENGINEERING ATTACK METHOD ON ICT SYSTEMS USING USB STICK

Goran Kunjadić[1],
Marina Savković[1],
Suzana Radović[2]

[1]Singidunum University, Belgrade, Serbia
[2]"Mr Consultant"

Abstract:
The use of methods of social engineering is a significant threat to the security of ICT systems. There are different methods of social engineering that can be applied depending on the means used. The main drawback of used methods is that the attacker comes into contact with the victim, usually in person or through various social networks. The method that we tested is based on the use of USB memory that is very effective, and there is no contact between the attacker and the victim. Taking into account the results of this study it is possible to improve safety awareness of employees and prevent or reduce the effects observed to attack ICT system.

Keywords:
Engineering, hacking, scripting.

1. INTRODUCTION

In this paper we are going to present a combined attack to ICT system. Information systems are constantly exposed to different threats including threats of using social engineering methods from the attacker. Different methods of social engineering (SE) are used but with the same goal. Attackers are trying to induce someone who has legal right to access the system to do some actions that will compromise the system. In this text we will use SEPF model to explain reasons of social engineering success based on socio-psychological factors. After that the attacker is going to exploit created vulnerability for unauthorized access to the system and compromise data or system as a whole. It is easy to imagine how much damage could be done to the system by the attacker if he succeeds to access the system in an uncontrolled manner. If using social engineering methods, attacker can use different approaches to the victim which will be described in the text. The attacker usually uses online approach which means that attackers have to bypass many network security measures including: firewalls, antivirus and antimalware software, intrusion detection system and so on. This is not an easy task and sometimes it is virtually impossible. From the other side attacker can also use a personal approach to the victim. The probability of success depends on the victim's psychological characteristics and profile as well as on the attacker's capabilities and skills. The main disadvantage of personal approach is that the victim could recognize the attacker later on. The method that we are testing doesn't require personal

Correspondence:
Goran Kunjadić

e-mail:
gkunjadic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2017-35-39

contact and there is no need for bypassing the network and system obstacles. The attacker considers conditions and circumstances under which the victim will take unsecured USB memory stick and plug in USB into the computer. A different kind of auto run malware could be implemented on USB. In the paper we will present a real tested case which was unexpectedly successful.

2. SOCIAL ENGINEERING - METHODS AND GROUNDS

SE is a phenomenon closely connected to dynamic technological changes. We can define it as a psychological manipulation of people with the intention to take advantage of their personal or organizational data. Common aims of SE attacks are: information gathering, fraud or system access. Usual elements of most of SE activities are: intended influence on users and human error or weakness that enables success of SE attack. In nearly 90% of incidents success of SE attacks are based on human faults or biases in decision making which lead to breaking standard security procedures [1] [10] .

Cialdini defines six principles used by SE attackers when they approach their victims: authority, commitment and consistency, reciprocity, liking, social proof and scarcity. Authority as a SE principle addresses people's habit to comply with authorities, even when they are persuaded to behave in a way different than their own beliefs [9]. Commitment and consistency are used by social engineers when they persuade behavior of a victim based on its identity, strong personal beliefs and habits [9]. In this case social engineers assume relatively predictable behavior of victims.

Reciprocity is based on a social norm that motivates people to compensate material or immaterial value received from others. Liking is an influence principle based on people's need to create and maintain social relationships. People have positive attitude towards others, so they could be „liked back". In a case when attackers show positive emotion towards a victim, they expect reciprocal reaction. Social proof is based on someone's need to be socially accepted. It can also be demonstrated in the case of alike opinions, when people trust others without any other reason. This principle is especially important in the case of decision making with high risk of loss. It is also successful in the case of relatively closed social groups with high level of mutual trust among their members. Finally, scarcity as a principle increases subjective value of goods or services, so it is a strong influence principle that can be used by a social engineer attacker. If something is relatively rare, a person will tend to perceive it as more valuable. It influences individual tradeoffs and approach to risky situations. Our example of SE attack is based on scarcity as principle of influence.

3. EMPLOYEES AS VICTIMS OF SE ATTACKS AND ORGANIZATIONAL *SE* VULNERABILITY

On corporate level, SE targets are employees, but the purpose of attack is reaching organizational resources or damaging organizational image for economic and non-economic reasons. Human, organizational and demographic factors can make an organization more or less vulnerable to SE attacks. Over 40% of security officers think that the greatest security threats in companies are employees who accidentally jeopardize security through data leaks or similar errors [10]. Social engineering focuses on weak spots of employees' behavior and habits and use it to avoid or break cyber security systems. One of the methods that can be used for organizational SE vulnerability assessment is penetration testing. Penetration testing (pen test) is a practice of checking IT systems that SE attackers could misuse. There are three main types of pen tests:

- Black box penetration testing,
- White box penetration testing and
- Grey box penetration testing.

In the case of black box penetration testing a tester has no information on the system he needs to test. The aim of the mentioned attack is gathering information on the tested system. However, White box penetration testing provides a wide range of information on system or network that should be tested (IP addresses, codes, schemes etc.). It simulates internal attack carried out by employees. Grey box penetration testing provides limited information to the tester. It can simulate external attack by someone who has already collected certain organizational security information. Grey box penetration testing is considered to be the best testing option if the tester is an external subject, considering cost/benefit analysis and security protection of potential information misuse risk.

Humans are the weakest link in the security chain so the security awareness program is of great importance while implementing security policy in the company. Correctly implemented security awareness program supports the organization with training, supervising and continuous improving of security awareness in the organization. Security awareness training should be composed of the following elements [6]:

- Organizational Security Awareness.
- Security Awareness Content.
- Security Awareness Training Checklist.

4. SOCIO-PSYCHOLOGICAL FACTORS OF SE ATTACKER-VICTIM INTERACTIONS

Social Engineering Personality Framework (SEPF) [9] can be used for analysis of SE victim's behavior. It explains socio-psychological factors that enable specific influence principles successful in SE interactions. We use it to connect different kinds of SE attacks with personal traits of victims. In the SEPF model, Cialdini's principles of social influence used by social engineers are matched with the Five-Factor Model (FFM), also known as the Big 5 [5].

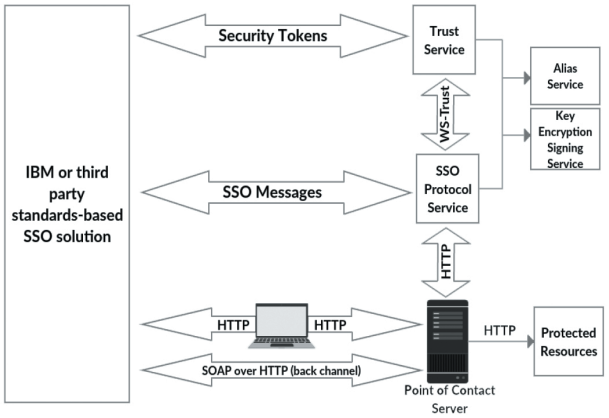

Fig. 1. SE Personality Framework (SEPF), [9]

FFM consists of five broad personality dimensions or traits that can be further split into several sub-traits. Conscientiousness is related to continuance commitment and focuses on: competence, self-discipline, self-control, persistence, dutifulness and following standards and rules. Extraversion is related to positive emotions, sociability, dominance, ambition and excitement seeking. Extraverted people are seen as highly vulnerable to SE attacks since they are more likely to violate cyber security policies [4] [9].

Agreeableness is also connected to a high level of SE vulnerability. Phishing is a SE method which particularly addresses this personality trait [3][9]. Agreeableness decreases a chance of breaking IT security rules, so overall SE vulnerability cannot be easily evaluated. Openness to Experience is related to influences approach to general IT security risk. Openness as a trait influences someone's risk evaluation so they are easily becoming SE targets [9]. At the end, neuroticism is seen as the least vulnerable personality trait in this case. According to SEPF model, neurotic individuals are more ready to respect cyber security policies. They are also more sensitive towards privacy issues, so neurotic persons are not seen as easy targets of SE attackers (Figure 1).

In the SEPF model, all influence principles are connected with specific personality traits, categorized through standard „Big 5" classification (FFM), shown in the Figure 1. The given influence principles are specifically successful in interaction with victims who have related personality traits. For example, extroverted persons are vulnerable when attackers use liking, social proof and scarcity as influence principles. Contrary to it, neuroticism is not connected with any given influence principle. If SE attackers are aware that some personality traits are more vulnerable to certain kinds of influence, they will be able to adopt their strategies and be more successful with their attacks. On the other side, this model can be used to design cyber security systems in groups or organizations, based on personality traits of its members or employees.

5. EXPERIMENT DESCRIPTION AND RESULTS ANALYSIS

A security assessment project, which was launched because of massive data leakage from a company, will be explained here. Security testing was performed in a Company which deals with tourist and hospitality industry. The company has 50–100 employees and it is placed in Johannesburg, South African Republic. The Company has three main organizational parts:

1. Department with tourist agents that communicate with clients.
2. Administrative and support department.
3. IT department.

Several activities were taken, including some forensic methods and engagement of the security forces. One of the segments of testing was testing by using SE methods. SE was an introduction step for Grey box penetration testing and breaking attempt into corporate IT system. Top management of the Company was completely informed about investigation and testing activities, but employees didn't have any knowledge about the testing itself, neither about the methods that were taken. The only technical person who was informed was the chief of IT and he was required to keep information confidential until testing was completed.

Department	Number of employees In %	Structure of employees by Education in %		Structure of employees by Sex in %		Number of USB sticks taken	Number of plug-in attempts
		University degree	High school	Female	Male		
1	73	39	34	51	22	5	7
2	23	11	12	18	5	3	5
3	4	4	0	0	4	0	0
Total	100	54	46	69	31	8	12

Table 1. Structure of employees and number of USB sticks taken

Several activities were taken, including some forensic methods and engagement of the security forces. One of the segments of testing was testing by using SE methods. SE was an introduction step for Grey box penetration testing and breaking attempt into corporate IT system. Top management of the Company was completely informed about investigation and testing activities, but employees didn't have any knowledge about the testing itself, neither about the methods that were taken. The only technical person who was informed was the chief of IT and he was required to keep information confidential until testing was completed.

Like preparation for testing, the testing team got layout of the building and access paths for pedestrians/employees. The testing team also got information about the environment: bushes, trees, flower pots, lamps and other objects near the access paths. At the same time the team purchased ten USB memory sticks, from different manufacturers and different shapes and colors.

The next phase was installing auto run script to USB memory, invisible for the user. The script was designed to PING the server, and let server know that it is present in the system. If a real attack was launched, the script would be malicious and harmful [2][8]. Also, some insignificant documents, pictures and video clips were placed on USB sticks as well. In the final phase of preparation USB sticks were sanded a little bit to look like used. After that USB sticks were placed at carefully chosen places near the access paths as it had to look like somebody dropped them accidentally. Placement of USB was done before working time and before employees started arriving to the Company.

Eight USB memory sticks were found and plugged in company computers 60 minutes after the morning shift had begun. Five employees plugged USB once, two employees plugged in USB twice and one employee plugged in USB three times. The largest amount of USB memory was taken by male employees with University degrees although female employees were the majority in the company. The three time attempt of plug-in was done by mail. Nobody from IT department either took USB or plugged in USB into Company computer.

Management of the Company was informed about results and had in mind that there were no bad intentions of the staff. The testing team suggested to management that two main types of measures should be taken:

1. Improvement of knowledge and security awareness of employees
2. Technical measures for limitation of using USB.

Technical measures were relatively easy to implement but working with employees was and still is a long term process of rising security awareness.

6. CONCLUSION

Employees are the weakest point of a corporate cyber security system, which is confirmed with our example. We can conclude that IT proficiency is connected to IT security awareness. In our case IT staff did not fail penetration testing since they had high level of security awareness. Other employees were not aware of security awareness and potential damage which could be done.

Also, some other employee characteristics influenced their behavior during the penetration testing. According to the analyzed SEPF model, scarcity as influence principle used by SE attacker is especially appropriate for people with high level of extraversion and openness to experience. All of the employees who were SE victims came from Sales department of the Company. It is consistent with evidence of our penetration test.

The most important is analysis of components of successful SE attack in the observed case. The reason of such behavior of employees is given in detail in the text and briefly in the conclusion. Having in mind the explanations and results given in this paper, Company management can significantly reduce the possibility of similar attack. It si certain that technical security measures have to be

implemented. In the observed case, USB memory stick has to be limited to the official devices with defining permission of the employee's right. Also, the Company should implement a customized employee security awareness training program. Since level of SE vulnerability in an organization is influenced by various factors including employee's characteristics, security awareness trainings for employees should be industry, profession and personality sensitive.

REFERENCES

[1] A.O. Adewole, A.E. Durosinmi Social Engineering Threats and Applicable Countermeasures. Afr J. of Comp & ICTs. Vol 8, No. 2., 2015, pp 177-180

[2] I.Oliver, J. San Jose, Systems and methods for detecting malicious code in a script attack, US Patent: US8839428 B1, Symantec Corporation, 2014

[3] J. L. Parrish Jr, J. L. Bailey, and J. F. Courtney, "A Personality Based Model for Determining Susceptibility to Phishing Attacks," Little Rock: University of Arkansas, 2009

[4] M. Warkentin, L. Carter, and M. McBride, "Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies," in The 2011 Dewald Roode Workshop on Information Systems Security Research, 2011

[5] R. B. Cialdini, M. R. Trost, and J. T. Newsom, "Preference for Consistency: The Development of a Valid Measure and the Discovery of Surprising Behavioral Implications," Journal of Personality and Social Psychology, vol. 69, 1995, pp 318–328

[6] Security Awareness Program Special Interest Group, PCI Security Standards Council, PCI Data Security Standard (PCI DSS), v1.0, Best Practices for Implementing a Security Awareness Program, October 2014

[7] Software Engineering Institute, Unintentional Insider Threats: Social Engineering, Carnegie Mellon University, 2014, available on: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdfI.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[8] Steinmetz, Frieder, USB - an attack surface of emerging importance, Technische Universität Hamburg, 2015, DOI: 10.15480/882.1283

[9] S. Uebelacker, Susanne Quiel, The Social Engineering Personality Framework, Socio-Technical Aspects in Security and Trust, IEEE Xplore, 2014, DOI: DOI 10.1109/STAST.2014.12.

[10] Verizon, Data Breach Investigation Report 2016, available on: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf