Social Engineering intrusion: A case study

Miika Sillanpää
Institute of Information Technology
JAMK University of Applied Sciences
Finland
miika.sillanpaa@optimesys.fi

Jari Hautamäki†
Institute of Information Technology
JAMK University of Applied Sciences
Finland
jari.hautamaki@jamk.fi

ABSTRACT

Social engineering is a very old method to influence people in their daily actions. The same methods added with new techniques have been implemented to create effective penetration mechanisms against organizations. The goal in this study was to measure employees' security awareness and culture. This is a case study which uses several penetration methods to test an organization's vulnerability against social engineering techniques. The study started with cyber security research questions for all employees in the studied organization Reconnaissance and survey questions together provide use cases to the physical penetration testing phase. When comparing the results of the survey questions with the actual penetration test, a significant difference was found. Even employees understand how to behave in a penetration case; they act differently. This is a problem which can be resolved by increasing the awareness against security engineering attacks. The awareness can be increased by training, education and good security policy.

CCS CONCEPTS

• Security and privacy • Social engineering attacks • Human and societal aspects of security and privacy

KEYWORDS

Social engineering, Information security, Cyber security, Intrusion Detection

ACM Reference format:

Miika Sillanpää and Jari Hautamäki. 2020. Social Engineering intrusion: A case study. 1, 1 (June 2020), 8 pages

1 INTRODUCTION

Social engineering is as old as human history and has been used many different way includng written form, non-verbal and oral forms[7, 12]. It is still a powerfull intrusion method and offers a potential attack vector. Specifically, this becomes concrete for BYOD devices (Bring Your own Device)[9]. Defence against social engineering attack is even harder than against normal attacks using information technology in different forms[2, 4]. A social engineer is one of the simplest ways to gather information about the target organization and their employees to exploit human vulnerabilities and protect against attack[3].

Social engineering refers to various methods by which a user of an information system can be manipulated to act in the manner desired by a manipulator[11]. Parallel terms for social engineering among others are user manipulation, social influence, and social hacking[5, 10]. There is nothing unusual about social engineering. It is part of our daily lives; children try to influence parents to get through their own will, or employees try to influence their supervisors to get a pay raise. Common to all forms of social engineering is the control of human behavior by attempting to manipulate them to accomplish the actor's will. In information security, social engineering seeks to influence the target person in order to gain unauthorized access to the target information systems and the information itself.[1, 14, 16] Social engineering intrusion can be seen as a set of different methods which use several tools and application in reconnaissance and physical penetration. Methods varies depend on the target organization. In this paper has been introduced one case study based on real organization.

1.1 Motivation and Structure

This study has been conducted in collaboration with a real organization [14]. Organization is a big finnish public company whose employers number is almost two thousand and revenue almost one billion euros. The aim of this study was to find out how the employees of the target organization react and act in situations of social engineering attacks. In the the organization has done regulary security audits and its own red team has conducted physical penetration testing. The results of this study give another point of view to asses how good the information security situation in the organization are and how it can be improve. The study was initiated by collecting background information about the organization using Maltego software from public information sources. The goal of gathering background information was to find out what information all potential attackers could find from the public sources. Information on how employees understand the content of information security, what is their awareness about information security and the organization's information security policy was collected through a survey. The questions of the survey were addressed to the all members of the staff in the entire organization. The scenarios were created based on the background information and survey. The purpose of using scenarios was to clarify how different physical intrusion methods would be influence for employee's behavior in different test situations. In addition, it was tested how workers reacted to physical intrusion. The aim was to find out if there are differences between the actual behavior and security knowledge. Figure 1 below illustrates how the different methods used in the study were combined in the implementation phase of the study.

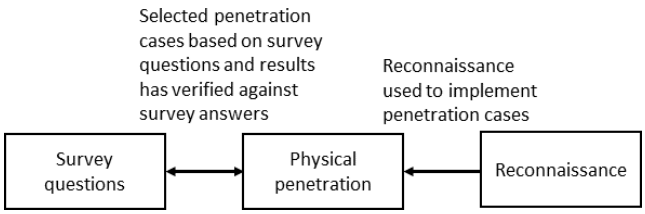

Figure 1: Interdependencies between research methods

The paper is organised as follows. In Section 2 introduce results from the survey, public information gathering and physical penetration. Lastly, we conclude our study in Section 3.

2 RESULTS

2.1 Survey questions on employees' security awareness

This survey measured the awareness of the organization's personnel regarding social engineering attacks. The survey contained 14 question and covered most common social engineering attacks[13]. The questions are listed below:

1. Do you use a strong password for work related systems, such as your workstation, to log in?
2. Do you use the same password for a variety of services such as Facebook or Instagram?
3. Do you use the same password to log in work related systems, such as workstation, and some personal services e.g. Facebook?
4. You are working on your workstation and the fire alarm goes off. What do you do in that situation?
5. Do you have or does your computer have any valuable information that might interest a hacker?
6. Your manager calls you from an unknown number. He is ill at home and his voice is about to go away and you do not know exactly what he says. He immediately needs the team's three most recent meeting reports and those should be packaged in one file, encrypted and sent to his private email (firstname.lastname@hotmail.com). The number your supervisor is calling from belongs to a member of the family. He has forgotten the computer and the phone on the previous day at work, cannot pick it up and these reports must go through asap. You can send the password for the compressed file as a text message to that number. What do you do?
7. You have plenty of data on the computer that you should save. Network does not work, so you cannot save the data on the network. You need some external media to store your data. You do not have enough large enough media for information. However, you notice a USB stick on the unused table next to you and you will notice that it so big that all the data will fit to it and there will be still space left. What do you do?
8. You are coming to work, and you will discover an unknown man in a suit with a computer briefcase in hand coming after you to inside smiling and thanking you. What do you do?
9. You get a call. The caller is from a research institute where a research has been purchased by the organization related to the personnel; identify strengths and areas of development and utilize information when designing development activities. The study is carried out on the telephone. A prize is awarded to the recipients. Do you answer the following questions about the research?
10. Your friend comes to you. He has problems with the network, and he should be able to retrieve some documents for a review. He has the rights to such documents. He has a USB stick that can be used to store the documents so he can access them. The stick is found on the top of the cabinet. How do you handle it?
11. You are coming to work in the morning. You will find that an unknown person is trying to get inside using his own card; however, the card will not work, and the doors will not open. What do you do?
12. You get a call. The service desk is calling. Virus software has detected a malicious program on your computer, which may be a ransomware, which, when activated, would encrypt all the data on the computer and therefore no access to them anymore. Malware can be removed but it must be done manually by remote access. There is a problem with the Service Desk workstation and there is no normal remote connection, so you should install another remote access software from the Internet, and this does not require any rights. He asks to download this to get remote control with the machine and remove this malicious program. What do you do?
13. You receive an email from your co-worker. The headline is "Look at this! Make your day much better!" The email has a Youtube link and additional text that says, "the best laugh this day". What do you do?
14. You are going to a cafe in the canteen and you notice a person walking toward you and you cannot see an ID card. What do you do?

A total of 70 employees responded to this survey. Next, the summary of the survey is presented.[15].

61 % of the respondents use a strong password, which is a really good result. Troy Hunt report in his article, that 86 % of Pwned Passwords subcribers are using poor passwords[8]. 37 % of the respondents use the same password for multiple public sites or public services. This is slightly lower than usually. Weilin Han et. al. report in their study that 59 % of users reused password in multiple websites[6]. In this study, 10 % of the respondents use the same passwords in work related systems, such as rganization's workstation, and some personal public services e.g. Facebook. In the study by Weilin Han et al., the same number was 33+- 9 %[6]. During a fire alarm, 96 % of the respondents lock their orkstations and then leave their workstation. In a phone call social ngineering case, 77 % of the respondents start different ways to confim the indentity of the caller. 70 % of the respondents do not connect an unknown USB memory stick to their computer. 83 % of the respondents don't let an unknown person enter through a locked door after themselves without the unknown person asking for permission. 97 % of the respondents do not answer the ID number question in case of phone call phishing. In a case where an unknown person is trying to get inside using his own card, 89 % of the respondents check the key properly and make sure it is not fake, advising the person to check their card and its rights. In the case of

phishing email 51 % of the respondents verify an email, and 3 % of the respondents trust a co-worker and open it. 26 % of the respondents ignore that email. 20 % of the respondents report phishing emails.

2.2 Information gained from publicly available medias

In this study, information is gathered from the assigner organization, and only passive gathering is used, e.g. Google, a website and Maltego. Information is also gathered from the ISP operators and cross-analyzed. The information from the website is reported in Table 1; from Google in Table 2, and from Maltego application and Shodan service in Table 3.

Table 1. Information from website

Organization	Operator
Personnel names and job titles	Some names of personnel, their job titles, images and phone numbers.
Organization structure and images	Organization structure and images
The main business plan and another job inside of the organization; what is their field of business?	Core business and expanded business from subsidiaries and their names
Charity area and couple of charity customers	Some startup companies that the operator has helped
Organization address	Organization address.
Emails addresses (e.g. helpdesk) and phone numbers	Helpdesk and other numbers. Also, many different email addresses.
Social media links	Social media links
Structure of email address	Structure of email address
Annual and other reports	Many annual reports that may give more information

Table 2. Information from Google

	Organization	Operator
Images	- Google images where there was a text about a new tablet and its model - Personnel ID card almost readable	- Images with personnel ID card visible
Normal search	- Information about a new service provider - Operator who operates all organization's network of places of sales	- Customer name and what services are included - Partners who help to develop a new mobile network
Domain Name System (DNS)	- Internet Protocol (IP) address space range - Public DNS names and IP addresses - Public mail servers and IP addresses - Persons' names - Many subdomains	- The same information
Advanced Google search (files etc.)	- Many PDF files, however, no useful information found	- Many PDF files and other files, no crucial information.

Table 3. Information gained from Maltego and Shodan

Domain (Search syntax: organization.fi)	- DNS names, Subdomains (syntax: text.organization.fi), Email addresses, Personnel names, IP addresses, MX and NS records, Phone numbers, Web sites and other subdomains
DNS names	- IP address of DNS servers - Information, how all different DNS servers link to each other. - Services that belong to that DNS server such as web sites. - Subdomains found (syntax: text.organization.fi) - More DNS names found
Subdomains	- Subdomains linked together, NS records, Email addresses, Phone numbers, More DNS names
MX and NS records	- Domain names, DNS records, IP address blocks
Websites	- Websites' titles - Technology and relationship
Public IP addresses	- Domain names, Services/port numbers, Email addresses, IP address ranges, Personnel names, Phone numbers, Other organization's information before merging together, IP address blocks (not organization's own), Hash values

2.2 Physical penetration testing

Physical penetration testing or pen test seeks to carry out real-world threat vectors that can be attempt to break the physical barriers of the organization. The aim is to gain access to the various functions of the organization, such as the information itself, the networks and the employees. The purpose with pentest is to assess the risk associated with potential security breaches. [17, 18] Physical penetration testinghas done using cases based on the survey questions.

First case included two different scenarios. The first scenario was carried out five times on a single day in about three hours' time slot. The other scenario was done four times; however, on different days and a different time of day. The case has been summarizex in Table 4.

In second case used a fake ID card. Personal informations to ID card, like name, photo, logo and job title in organization, was founded from website in gather phase. Case executed six times and at a different time and on the different day to get more statistics. In the Table 5. has summarized these attemps.

Third case was almost the same as first case 1 except in this case author did not even try to hide a possible ID card. This case was performed twice over three days. Table 6. summarize this case.

Table 4. Scenarios and results from Case 1

Scenario	Time	Breaching point	Success rate (attempts/successful)	Information about breach
1.1	Morning when employees come to work. (7.30 am – 10 am)	Personnel main entrance	3/3 Success	No questions asked and not looking behind. Not trying to get any floors.
1.2	(7.30 am – 10 am)	Side door	2/2 Success	Getting inside via stairs and elevator to the floors with "helpful" employees.
2.1	Morning (8 am)	Car garage	1/1 Success	Through car park to the building and onto the floor in the elevator with employee.
2.2	Midday (10 am)	Personnel main entrance	1/1 (tailgating) Success 0/1 (moving without ID badge) Failure	Tailgating inside and onto other floors. Got caught by an unfamiliar employee on the floor.
2.3	Morning (7.30 am)	Personnel main entrance	1/1 Success	Tailgating to the building and then with another employee onto the floor in the elevator.
2.4	Morning (about 7.30 am)	Side door	1/1 Success	Un-familiar employee opened the door from inside and let me pass. Used elevator with other employees and got onto the next floor. No questions or any verification asked.

Table 5. Results from Case 2

Attempt	Time	Succeed (F) or or Failed (F)	Information and summary
1.	11.30 am	S	Receptionists were deceived by the fake card.
2.	7.30 am	S	An employee opened the door and helped to get to the first floor in the elevator. The ID card was not checked.
3.	9 am	S	The side door was used through which access was gained to the floor in the elevator with an employee. The employee took a closer look at the card but did not ask to see it better.
4.	8 am	S	Floor accessed via an elevator. The employee did not look at the ID card at all.
5.	8 am	S	The ID card was not looked when access inside was gained. The floor was accessed with another employee.
6.	9.30 am	F	Very good security behavior from one of the consultants. Very sharp eyes, good questions to verify the ID and information given to the security team.

Table 5. Results from Case 3

Test scenario	Duration	Information about attempt
1.	1	Moved from end to end on the floors. Greetings from familiar employees but no questions or other interruptions. Tailgated sometimes to another floor.
2.	2	Same as above but duration was longer.
Related to the case 1 breaches and their information	4	No interruptions when walking. Only got caught once by unfamiliar employee.

2 CONCLUSIONS

The questionnaire provided the baseline about the personnel's security culture and awareness. The survey showed that there is no perfect organization, security action or perfectly implemented security equipment and practices. There is always some way that can be used to launch an attack. The personnel's safety behavior and security culture situation in an organization among the staff representatives who participated in the survey was overall good. Most of the staff would act at a good level in defending the organization and its assets from social engineering attacks. Still, there are people with a poor security culture that can be used to

penetrate physical spaces. Increasing training and situational awareness of cyber security threats is an effective method to decrease attacks by using social engineering. Most of the attendees were from the HQ of the participating organization. Based on the total number of all employees in the HQ, the error margin was about 9% with 90% reliability level.

There is a plenty of information (Table 1 and 2) can be found about the organizations. The focus in social engineering is on hacking humans; therefore, any information about an organization and its employees is useful. A successful social engineering attack needs a variety of background information about the organization. Such information includes e.g. the focus of the organization's activities, contact information in different situations, and the personal information of the organization's employees. The perpetrator of the attack can build a fairly good picture of the situation using the collected data. This information is used to plan the attack. The Google search gave several good potential attack scenarios. Image searching gave one launched case; using a fake personnel ID card. All DNS information was also visible without any hidden information. The Internet DNS search with Maltego and Shodan information (Table 3) together provided plenty of data. The information shows how all public services link together as well as their IP addresses.

The success of tailgating depends very much on the security behavior and culture of the personnel. The personnel are the first line of defense against physical penetration and social engineering. As in Table 4 summary, over 80% would stop an unknown person and ask who he/she is and where their ID card is. However, in the real act in case 1, the success rate was 10% when trying to get inside from outside and no questions were asked. Tailgating was also successful when continuing the penetration deeper into the building using stairs and an elevator. When comparing the survey results and the real act against physical penetration, we can see many differences. On paper, everything looked good; however, in the real situation people behaved differently. The most interesting result was that almost 90% of the respondents to the survey answered that they would examine an unfamiliar person's ID card. The reality was different. In the penetration test, none of the personnel (0/5) looked at the ID card. Also, all target persons in the penetration test used their own card to open the exterior door after the author said that the card is not working.

Training, education and security policy will help to accomplish this security behavior on how to handle and what to act with security threats. It would be beneficial and suitable to point out the social engineering techniques and attacks to the personnel in a real act and teach them some remediation and mitigation actions than just telling them to read all guides or watch some presentations.

In a summary, employees are the path inside an organization. Without a good security procedures, they are vulnerable
to attacks. The outside threat is easier to spot and stop. The insider threat is much harder to prevent.

ACKNOWLEDGMENTS

This research is partially funded by the European Union under the H2020 Programme Grant Agreement as part of the C*yberSec4Europe* project of JAMK University of Applied Sciences Institute of Information Technology.

REFERENCES

[1] A. S. Alazri. 2015. The awareness of social engineering in information revolution: Techniques and challenges. In 2015 10th International Conferencefor Internet Technology and Secured Transactions (ICITST). 198–201. https://doi.org/10.1109/ICITST.2015.7412088

[2] T. Bakhshi. 2017. Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. In 2017 13th International Conference on Emerging Technologies (ICET). 1–6. https://doi.org/10.1109/ICET.2017.8281653

[3] P. Engebretson. 2011. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Syngress Publishing.

[4] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh. 2016. Social Engineering Attack Strategies and Defence Approaches. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). 145–149.

[5] S. Gupta, A. Singhal, and A. Kapoor. 2016. A literature survey on social engineering attacks: Phishing attack. In 2016 International Conference on Computing, Communication and Automation (ICCCA). 537–540.

[6] W. Han, Z. Li, M. Ni, G. Gu, and W. Xu. 2018. Shadow Attacks Based on Password Reuses: A Quantitative Empirical Analysis. IEEE Transactions on Dependable and Secure Computing 15, 2 (March 2018), 309–320. https://doi.org/10.1109/TDSC.2016.2568187

[7] J. M. Hatfield. 2018. Social engineering in cybersecurity: The evolution of a concept. Computers and Security 73 (June 2018), 102–113. https: //doi.org/10.1016/j.cose.2017.10.008

[8] T. Hunt. 2018. 86 % of Passwords are Terrible (and Other Statistics). https://www.troyhunt.com/86-of-passwords-are-terrible-and-other-statistics/. Accessed: 29 January 2020.

[9] K. Krombholz, H. Hobel, M. Huber, and E. Weippl. 2015. Advanced social engineering attacks. Journal of Information Security and Applications 22 (June 2015), 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

[10] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter. 2014. Social engineering attack framework. In 2014 Information Security for South Africa. 1–9.

[11] F. Mouton, A. Nottingham, L. Leenen, and H. S. Venter. 2017. Underlying finite state machine for the social engineering attack detection model. In 2017 Information Security for South Africa (ISSA). 98–105.

[12] S. Nathaniel. 2018. The History and Evolution of Social Engineering Attacks. https://commissum.com/blog-articles/the-history-and-evolution-ofsocial-engineering-attacks/article/ Accessed: 27 January 2020.

[13] P. Paganini. 2019. The Most Common Social Engineering Attacks. https://resources.infosecinstitute.com/common-social-engineering-attacks/#gref Accessed: 23 April 2020.

[14] S. Sabouni, A. Cullen, and L. Armitage. 2017. A preliminary radicalisation framework based on social engineering techniques. In 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). 1–5. https://doi.org/10.1109/CyberSA.2017.8073406

[15] Miika Sillanpää. 2019. Social engineering against security policy : How to infiltrate company's premises using social engineering ? Master's thesis. Jamk University of Applied Sciences, https://www.theseus.fi/handle/10024/265555.

[16] V. K. Singh, A. Mani, and A. Pentland. 2014. Social Persuasion in Online and Physical Networks. Proc. IEEE 102, 12 (2014), 1903–1910.

[17] S. Stankovic. 2019. Physical Penetration Testing Methods (That Actually Work). https://purplesec.us/physical-penetration-testing/. Accessed: 29 January 2020.

[18] G. Weidman. 2014. Penetration Testing: A Hands-On Introduction to Hacking. Books24x7.