Social Engineering

Pedro Mauricio Tavares, Dublin, Ireland

***Abstract*—There are several methods that malicious individuals can use to try to breach security systems in an organization. Social Engineering is one of them and one of the most efficient.**

Companies invest a large in technology but they often forget about a crucial factor that will make a huge difference in their security system, the human factor. Social Engineering explores this vulnerability. Because of their investment in security do not follow their growth, the main target are big companies, according to a research done in USA in 2002.

The goal of this paper is to provide and describe, in a high level and detailed way, a topic of my choosing, namely Social Engineering, which is arguably one of the most powerful ways to gain access to your target's information assets.

In this paper, we will explore what Social Engineering is, its cost to the organization, some of the techniques that are used to conduct Social Engineering attacks and some of the methods used in order to take advantage of human behaviour. The paper also discusses some ways to prevent this kind of attack, highlighting the importance of a security policy and education.

Furthermore, this paper provides a section about punishment issues when dealing with Social Engineering and will also show a related work review.

In the last part, we will raise some questions and discuss what and how they can influence us for future research.

***Index Terms*—Motivation, Problem, Approach, Social, Engineering, Hacker**

I. Introduction

WE must work together to understand the enemies' processes and procedures to ensure that we can properly prevent their damaging and malicious behaviour.

Malicious hackers are constantly looking for ways to gain access to valuable resources such as computer systems or to obtain information that can be used by them for personal gain. Sometimes they get their chance when there are genuine gaps in the security that they can breach. A huge amount of loss has been suffered by organizations and individuals because of these attacks.

Social Engineering attacks neither give a specific formula nor a single method, they consist of physical and psychological aspects. In the physical aspect, the working place, trash etc. are explored. In the psychological one, they deal with the feelings and sense of trust of people.

In short, they use human weakness in order to gain access to any system despite the layers of defensive security controls that have been implemented via software or hardware.

II. What is Social Engineering?

People are considered the weak link in an Information Security System, Social Engineering is the art of exploiting such a link [2]. Social Engineering is “people hacking” and involves maliciously exploiting the trusting nature of human beings.

In addition, Social Engineering is one of the toughest hacks to perpetrate because it takes courage and skills to come across as trustworthy to a stranger. It is also more challenging to manage since it depends on human behaviour and involves taking advantage of vulnerable people[3].

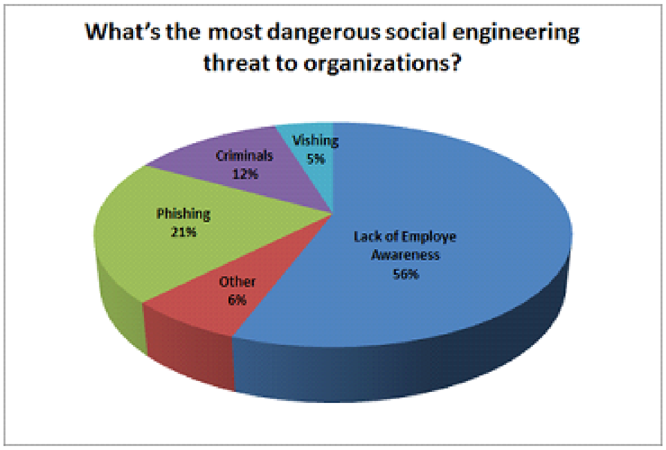

Fig. 1
Social Engineering threats [1]

A. Impact of Social Engineering on the organization:

In order to keep in business nowadays, Information Security is essential for any organization. If Information Security is not given priority, any or even a small gap in security can bring an organization down.

The financial cost could be punitive to the organization and to the individual. So much so, that insurers are now beginning to cover losses arising out of some kinds of security breaches [4].

To make you aware of how much cyber-attacks cost, think about the USA where cyber-attacks cost companies $266 million last year - more than double the average annual losses for the previous three years, according to a report released by the San Francisco-based Computer Security Institute (CSI) and the San Francisco FBI Computer Intrusion Squad. The study found that 90% of 273 respondents detected some form of security breach in the past year. Besides, there is also a loss of reputation and goodwill, which can erode a company's base in the long run [5].

Security experts have come to the conclusion that the majority of violations are caused by either discontent employees or non-employees who have legitimate system ac-

[1] Source: `http://www.darkreading.com`

cess because of their role in the organization. According to the FBI nearly 80% of all attacks are caused by such authorized users.

Social Engineering is a very effective and very easy method of getting around security obstacles. A successful Social Engineer is when they extract information without raising any suspicion.

III. Targets

If we analyse in detail, it will be hard to find someone or some company that has not suffered a Social Engineering attack. Who hasn't ever been fished by someone and by the time the person realizes what is happening, has already given up valuable information? Sometimes, the person never even realizes that they have given up information.
We can cite a few examples, like a job offer that we are interested in but by the time we go there, "our" colleague already took the position; or when we have a good deal to make in order to sell something, another person whom knows you got there before you.
Because of these examples previously mentioned, we sometimes ask ourselves: "How did he know about it?" But then, we forgot the couple of drinks we had in the pub where we mentioned something without intention.

The situation is similar when the targets are large companies, financial institutions, military, government agencies and even hospitals. However, these attacks involve more prepared and skilful people. Normally, a Social Engineering attack has a low cost and is very efficient, so much so that most of the companies do not perceive that were attacked and even if they discover they were attacked, they hardly admit it because they don't want to tarnish their reputation.

IV. Ways of Attack

The ways of attack vary, from Direct Approach to Dumpster Diving, nevertheless it always exploits the weakness and naivety of people.

No article about Social Engineering attacks would be complete without mentioning Kevin Mitnick, one of the greatest hacker of all times. From an interview for the BBC, Mitnick said: "The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you. What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time organizations overlook that human element" [6].

The process of Social Engineering is actually pretty basic. Generally, Social Engineers discover the details of organizational processes and information systems to perform their attacks. With this information, they know what to pursue. Normally, Social Engineering attacks are in four simple steps:

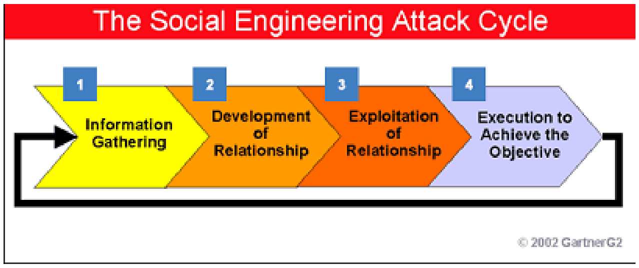
The Social Engineering Attack Cycle
1
Information Gathering
2
Development of Relationship
3
Exploitation of Relationship
4
Execution to Achieve the Objective
© 2002 GartnerG2

Fig. 2
Attack Cycle [2]

These steps can include numerous sub steps and techniques, depending on the attack being performed [7].

A. *Information Gathering*

After Social Engineers have a goal in mind, they typically start the attack by gathering public information about their victim(s). Many Social Engineers acquire information slowly over time so they don't raise suspicion.

A.1 Online

Perhaps the most basic research medium is the Internet. A few minutes searching on Google or other search engines, using simple keywords, such as the company name or specific employees' names, often gives you a lot of information. By using this search-engine information and browsing the company's website, the attacker often has enough information to start a social engineering attack. Jobs websites are a good example if you want to find out information about the target company.

In the case of finding information about people, the use of Social Networking such as Facebook or LinkedIn is very useful. The information collection is made even easier for you because you can search by company name to find past and present employees of your target. You might also find a group for current and ex-employees of a company or a person's workmates. In addition, the posts posted by the victims, can also be used for demonstrating insider knowledge when striking up a conversation with your target [8].

A.2 Dumpster Diving

Dumpster Diving is a little more risky and sometimes messy. Nonetheless, it's a highly effective method of obtaining information. This method involves literally checking through trash bins for information about a company. This method can bring about a lot of confidential information because many employees assume that their information is safe after it goes into the bin.

The Social Engineer may look for documents such as phone lists, employee handbooks (which often contain security policies), network diagrams, meeting notes, reports and so on.

[2] Source: http : / / defendersprotection . org /)

A.3 By Phone

Attackers can obtain information by using the dial-by-name feature built in to most voice mail systems. To access this feature, you usually just press 0 after calling the company's main number or after you enter someone's voice mail- box. This trick works best after working hours to ensure no one answers.

A.4 Phishing emails and Passwords

Passwords are the biggest weakness of companies. Many people use words that exist in dictionaries and also use passwords like their nicknames, or even their own names. According to Kevin Mitnick [3], this used to represent up to 70% of the total passwords within companies.

There are a few ways to perform phishing, a simple one is to set up a bogus e-mail account requesting information or linking to a malicious site, send e-mails to employees or other users you want to test, and see what happens.

B. Development of Relationship

Trust is the essence of Social Engineering. Most people trust others until a situation forces them not to. People want to help one another, especially if trust can be built and the request for help seems reasonable.

Most people want to be team players in the workplace and don't realize what can happen if they divulge too much information to a trusted source who shouldn't be trusted. This trust allows Social Engineers to accomplish their goals.

C. Exploit relationship

The hackers see Social Engineering from a psychological point of view, learning how to create the perfect psychological environment for an attack. The main object of persuasion is to convince the person who will give information that, the Social Engineer is indeed a person whom he/she can trust and provide information to.

Another important factor is never asking for too much information at the same time but do it slowly and use different people, in order to maintain a comfortable relationship.

A good way to get information during a Social Engineering attack is being friendly. The place to approach does not necessarily need to be in the company, it can be a club or a pub for instance. The hacker only needs to win the trust of the target employee, enough to convince him/her to provide "all requested help". Overall, most employees responds well to kindness, especially women. A smart hacker knows when to stop extracting information before the victim suspects themselves of being subjected to an attack[9].

V. **Ways to prevent**

The power of a Social Engineer should never be underestimated. We have only a few types of defence against Social Engineering. Even with strong security systems, a naive or untrained user can let the Social Engineer into the network.

Prevention of Social Engineering is not an easy task, the majority of companies do not direct neither financial resources nor people for that. They prefer to invest in new technologies rather than invest in measures to avoid Social Engineering. Because of these factors, there will be always a way to breach security using people as people's behaviour changes constantly.

In order to reduce such risks, there are a few measures we can take to mitigate these risks: A well-documented and accessible Security Policy. Training on the Security Policy.

A. Social Engineering Countermeasures

A well-documented and accessible Security Policy and associated standards and guidelines form the foundation of a good security strategy. The policy should clearly document in layman terms, its scope and content in each area that it applies to. Along with each policy, the standards and guidelines to be followed in order to comply with the policy should be specified[10].

Below are some of things the policy document should cover:

- Computer system usage – monitoring usage, the use of non-Company- standard hardware or software, response to chain mail etc;
- Information classification – Classifying information so that users don't have access to certain levels of information they don't need;
- Personnel security – screening new and non-employees to ensure that they do not pose a security threat;
- Information access – password usage and guidelines for generating secure passwords. Passwords should be required to expire after a specified period in all systems. Standards for secure passwords should be defined;
- Protection from viruses – to secure the systems and information from viruses;
- Information security awareness training and compliance – to ensure that employees are kept informed of threats and counter measures;
- Re-create and invalidate user IDs for employees, contractors, and consultants who no longer work for the organization;
- Reports: Responding to security incidents, such as suspicious behaviour;

These policies must be enforceable and enforced for everyone within the organization. Keep them up-to-date and tell your end users about them.

B. Education of the User

None of the policies and procedures above will be effective if the users were not trained in order to properly follow them. Training employees is the best line of defence to identify and respond to Social Engineering attacks. It begins with an initial training for everyone and then we align training and awareness with these security policies [7].

While employees are undertaking ongoing training and awareness in their organization, the following tips can help them to combat Social Engineering in the long term[11]:

- Never release any information unless you can be sure that the person requesting it needs it and are who they say they are. Always verify the caller's identity, if a request is made by the telephone;
- Never click an e-mail link that supposedly loads a page with information that needs updating;
- Be careful when sharing personal information on social networking sites, such as Facebook or LinkedIn;
- Never open email files from strangers;
- Never tell your password;
- Do not let a stranger use a device to connect to your network jacks or wireless networks.

VI. Punishment

Social Engineering attackers can be punished by the means of the common law in each jurisdiction he/she is trying to conduct the attack. For example, someone can be charged for getting into an unauthorized access building. But, is this enough? What about the employees that let such a situation happen?

Some Vendors claims that security can be improved if companies hold employees accountable for carelessly allowing different types of Social Engineering attacks to happen such as clicking on emailed links that lead to malware being downloaded to the companies' network [12].

KnowBe4 [13] claims that simply re-training employees who are prone to falling for phishing attacks is not enough to make workers really aware of the dangers. Rather than simply re-training, KnowBe4 advocates reporting those to immediate supervisors and human resource departments that can pressure workers into becoming more careful. Therefore, the employees will see a greater repercussion and consequently will change their behaviour.

KnowBe4 did a study on the employees of 372 companies over a 12-month period. Of the 291,000 people who underwent testing, the vendor found around 16% whom were prone to getting caught out on phishing emails. KnowBe4 claims that once the test group was held accountable for an attack, the percentage of those among the 16% becoming victims of phishing attacks again dropped to just 1%.

VII. Related work (Review)

A. Introduction

Social Engineering is a topic that raises attention from different people within the Computer Science and Security field. In this section I will briefly discuss a related article written by Malcolm Allen, whom is a certified analyst from the Global Information Assurance Certification(GIAC)[14]. His article is called "SOCIAL ENGINEERING: A means to violate a computer system"[15] and it is widely mentioned in different books when the main topic is Security in Information Systems [16].

B. Literary work

Allen's paper basically covers the security aspects of Social Engineering and has the purpose to act as a guide on the subject of Social Engineering, explaining how Social Engineering can be used in order to violate a computers system.

There are few things on Allen's work that is similar to this, our work, for instance, Allen begins giving a definition of what Social Engineering is and its cycles as we already mentioned in Sections 2 and 4.

Then Allen briefly discusses a topic that was not covered here, which is about the motivation for Social Engineering. The reason I preferred to leave it out from our research is because, in the computer field, the vast majority of different types of attacks to breach a system is motivated by the personal financial gain, therefore, this is not new or uncommon.

Throughout the explanation of the Social Engineering phases, Allen also talks about the main techniques of Social Engineering such as Dumpster Diving, phishing and so on. These techniques are worth knowing, therefore, in most articles or books they will be mentioned as we did in this paper.

In the last paper of his paper, Allen mentions the counter measures for Social Engineering and defines very briefly some of the controls such as Education, Physical security and Policy etc, which should be implemented for a company in order to try to prevent Social Engineering attacks.

C. Conclusion

Allen's article is fairly useful and I truly encourage people who want to start off learning about Social Engineering to read it. However, he should have gone a little deeper into some very important and crucial points such as policy and education.

Another thing that Allen did not mention but I thought that it was worth writing about was punishment for the people involved in Social Engineering attacks as I feel that any article about security breaches and crimes are incomplete if we do not mention it.

VIII. Conclusion

The vast majority of incidents and breaches in Information Security Systems count human intervention as a predominant factor. As we just saw in this paper, people and processes comes before technology in Information Security Systems. Having said that, there is no point investing millions in technology if the human factor is not taken seriously.

It is recommended that private and public sectors implement a centralized security policy and make sure that staff and employees will get a proper training around it. It is not about making people paranoid about security but to be alert, prepared against requests and being aware of the consequences of the information provided at which they are responsible for.

We could see in this paper how long Social Engineering have been around and how efficient it can be and, after having carefully researched in order to write this article, three questions are worth discussing:

In the next coming years, will Social Engineering still be the greatest threat for Information Security in companies?

It seems like, even with all the improvements in education and security policies, Social Engineering is still a powerful method for the hackers to penetrate security systems. It looks like this problem for security administrators will not have a "real" or 100 per cent solution in a short term period.

We also mentioned in this paper and showed an example of how security systems would be improved if companies began to punish the naïve staff who, by mistake, gave access and allowed a Social Engineering attack to succeed. But there are some questions and points we should raise for this matter: How far will the punishment go towards the careless employee?

As we know and mentioned in this paper, Social Engineering is not a specific tool or method but a collection of techniques of different parameters. Different situations will be performed during an attack. So, is it really fair to punish an employee that just behaved in the same way that every person would do if they were in the same situation?

If all companies start punishing their employees, how will they differentiate from the person who just clicked a malicious link to someone else who gently opened the door to a well-dressed individual, wearing the companies badge and who showed to know a lot about the company in a short conversation?

Having asked these previously two questions, a third one raises:

Is it the case that we will rely more on technology rather than on Humans in order to avoid Social Engineering attacks? Will machine learning be a key tool used to fight against Social Engineering? For example, could companies start to use security cameras together with machine learning algorithms in order to detect, by facial recognition, someone suspicious in the company, raising a security alert to a specific department? As we do not need to deal with different circumstances in machines, machine learning could be the key to solve the threat of Social Engineering in the future?

In conclusion, for now, Social Engineering tools are everyone's concern, the proper use and planning of these tools will make the difference, as the more prepared the employees of a company are, the more secure the company will be.

References

[1] Michel Goossens, Frank Mittelbach, and Alexander Samarin, *The Companion*, Addison-Wesley, Reading, MA, 1994.

[2] Huber M., Kowalski S., Nohlberg M., Tjoa S., *Towards Automating Social Engineering Using Social Networking Sites, Computational Science and Engineering, 2009, Volume: 3.*, Digital Object Identifier: 10.1109/CSE.2009.205, Publication Year: 2009, Page(s): 117 – 124

[3] K. Mitnick, W. Simon and S. Wozniak, *The art of deception. Indianapolis, Ind.*, John Wiley & Sons, 2003.

[4] T. Hoffman, *Security breaches. Viruses. Should you amend your IT insurance plan to cover such risks?*, Computerworld, 2003. [Online]. Available: http://www.computerworld.com/article/2581568/security0/premium-protection.html. [Accessed: 28- Mar- 2016].

[5] A. Harrison, *Survey: Cybercrime Cost Firms $266M in 99, Computerworld, 2000.*, [Online]. Available: http://www.computerworld.com/article/2593953/it-management/survey–cybercrime-cost-firms–266m-in–99.html. [Accessed: 28- Mar- 2016]

[6] BBC NEWS and Technology, *How to hack people, News.bbc.co.uk, 2002.*, [Online]. Available: http://news.bbc.co.uk/2/hi/technology/2320121.stm. [Accessed: 28- Mar- 2016].

[7] Kevin Beaver, *Hacking for dummies, 4th ed. Hoboken, NJ:*, John Wiley & Sons, Inc., 2013, pp. 70-77.

[8] A. Harper, S. Harris, T. Williams, G. Lenkey, C. Eagle and J. Ness, *Gray hat hacking, 3rd ed. New York:*, McGraw-Hill, 2011.

[9] S. Granger, *Social Engineering Fundamentals, Part I: Hacker Tactics", Symantec.com, 2001.*, [Online]. Available: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics. [Accessed: 28- Mar- 2016]

[10] G. Stevens, *Enhancing Defences Against Social Engineering,*, SANS Institute, UK, USA, 2002.

[11] S. Conheady, *Social engineering in IT security. New York:*, McGraw-Hill Professional, 2014.

[12] A. Gonsalves, *Punish careless employees to reduce security breaches, vendor says, CSO Online, 2014.*, [Online]. Available: http://www.csoonline.com/article/2134315/security-awareness/punish-careless-employees-to-reduce-security-breaches–vendor-says.html. [Accessed: 28- Mar- 2016].

[13] Security Awareness Training, *Compliance Software - KnowBe4, Knowbe4.com, 2016.* [Online]. Available: https://www.knowbe4.com/. [Accessed: 28- Mar- 2016]

[14] GIAC Forensics, Management, *Information, IT Security Certifications, Giac.org, 2016.* [Online]. Available: http://www.giac.org/certified-professional/malcolm-allen/102421. [Accessed: 29- Mar- 2016].

[15] M. Allen, *Social Engineering: A Means To Violate A Computer System, SANS Institute, 2006.* [Online]. Available: https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529. [Accessed: 29- Mar- 2016].

[16] S. Bosworth, M. Kabay and E. Whyne, *, Computer Security Handbook, Set, 6th Edition, New Jersey, USA:*, John Wiley & Sons, 2014.