SOCIAL ENGINEERING IN THE CONTEXT OF CYBER SECURITY

Toni NAUMOVSKI[1]
Nenad TANESKI[2]

Abstract

Social engineering, as an art of deception, is very present in the era of globalization and it intertwines with plethora acts of unfair activities. Managing of this risk is a significant security challenge. The paper analyses the social engineering as a big cyber security concern that harms productivity and efficient of any organisations. It is intended to cover the different aspects of social engineering and should be viewed as a study which identifies social engineering hazards. Besides the introduction given in Section 1, Section 2 defines term social engineering, in Section 3 the forms of social engineering are presented, Section 4 gives the guidelines to mitigate the risk of social engineering, and the last section contains the conclusion.

Key words: social engineering, manipulation, risk, confidential information, cyber security, organization.

Introduction

There is no way to be truly one hundred percent secure. The acts of many unfair manipulated activities that target the human behaviour unfortunately gain access to the system of any organization despite the different ways of established security controls and policies. This refers to the so called social engineering and that access is nothing else than deception. The gap of security or the hole in the “fence” regard to the employees’ naivety disrupts the survival of any organization. Manipulation, persuasion and framing people are hot topics nowadays. Security of any organization is very linked with the challenges deriving from the social engineering. The technical aspect of the security made much progress in recent years. It has been easier to make patch of technical nature, than human. For many organizations the weakness thread for the security is now the human and human are a “hole”, especially for the cyber security. Defining the phenomenon “social engineering” and forms of its manifestation, as well as good security policies and education at different layers should minimized the social

[1] The author, PhD, is Staff officer in the Army General Staff /MoD.

[2] The author, PhD, is Associate professor, Head of the Department of Military Science, Military Academy/MoD.

engineering appear and its influence on cyber security and should improve the risk management process.

The phenomenon "social engineering"

Manipulation and persuasion of people are the basis of social engineering and they easily affected people. Despite the technical aspects to the cyber security where large improvements are achieved, the same cannot be said for the human factor. While the focus of the vast majority of our security efforts are on protecting computers and networks, more than 80% of cyber attacks and over 70% of those from nation states are initiated by exploiting humans rather than computer or network security flaws. To build secure cyber systems, it is necessary to protect not only the computers and networks that make up these systems but their human users as well (Shen, n.d). So, the focus has been shifted to the employees. A true definition of social engineering is the act of manipulating a person to take an action that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action (Hadnagy, 2011). Hadnagy (2011) gives an example with doctors, psychologists, and therapists. He explains the difference between therapist and con man. In fact doctors, psychologists, and therapists often use elements of social engineering to "manipulate" their patients to take actions that are good for them, whereas a con man uses elements of social engineering to convince his target to take actions that lead to loss for them. Even though the end game is much different, the approach may be very much the same. A psychologist may use a series of well-conceived questions to help a patient come to a conclusion that change is needed. Similarly, a con man will use well-crafted questions to move his target into a vulnerable position. Social engineering as an attack vector makes interaction with humans by manipulating them and often breaks best systems and networks security procedures in order to gain access to the confidential information. The DIGITAL GUARDIAN recently has made review of the infosec experts who discuss the phenomenon social engineering. The article has been prepared by Nate Lord. Let's see what some of the experts said below:

- Creating a fake persona or using one's role in an improper way, is pretty popular for social engineering attacks. Social engineering is hard to prevent. That's the tough part (Peterson, 2019).
- Social engineers usually have their eyes on something bigger than their unsuspecting targets. The innocent victims are just a convenient and easy way for the cybercriminals to get to a bigger prize (Mancusi-Ungaro, 2019).

- Most of the cybercrime activity stems from massive infection campaigns that rely on mass scale social engineering (Shulman, 2019).
- Social engineering is generally used to widen an already existing breach of information. So for example, an attacker may have certain information about the employees within a company, and he uses that information to learn something new — for instance, a password to an internal system. Professional cybercriminals extract one piece at a time, slowly earning their way in deeper to the organization (Simione, 2019).
- The weakest link in a company is still the employees that work there. Attack methods are as common as they are boring (Maxwell, 2019).
- Social engineering attacks like phishing emails and identity theft are the most common cyber threats that companies face (Murashka, 2019).

There is no unique method that will ensure complete security against attack of social engineering. The types of attacks can vary, but when individuals/employees are targeted the social engineers usually, by trick, tries to get confidential information, or to get access to the network or computer system, to secretly install malicious software that will give them access to the passwords or other confidential information as well as giving them control over the whole network or computer system. Many employees do not realize the full value of personal data and are unsure how to protect confidential information. Any company/corporation, government, individual, or power can be destroyed due to a lack of knowledge (Evans, 2009:1). Evans (2009:12-13) states that social engineering is the exploitation of said vulnerability and there is no patch for human stupidity. It is a problem with no solution. About the nature of social engineering, according to Evans, the psychological aspect of social engineering is what makes the attack, not the technical. Peltier (2012), the author of several books on information security, highlights that the social engineer preys on qualities of human nature, such as: the desire to be helpful, the tendency to be trusting, the fear of offending others and the tendency to cut corners. This means that the social engineering attack is powered by psychology aspects of human behaviour. Employees in every single organization, as well in the military, who have access to valuable information, are the potential risk for that organization. So, they are the weakest link in the cyber security chain and as much as more employees are in the organization, the landscape of potential social engineering attack is much bigger.

Forms of social engineering

A social engineering attack can be targeted or opportunistic. Targeted attacks typically focus on a specific individual, whereas opportunistic attacks aim to glean information from anyone in a specific position (Samani and McFarland, 2014:6). Social engineering according to Samani and McFarland (2014:6) can be divided into two categories: hunting and farming. Hunting aims to extract information using minimal interaction with the target. Farming aims to establish a relationship with the target and to “milk” the relationship for information over a longer period. Other dimension has the psychological aspects of social engineering attack where an attacker misleads the people into doing something they want people to do. While the term social engineering is often used to describe all trickery used to manipulate people into performing actions or giving up information, the rapid development of electronic means of deception have led some security professionals to believe that social engineering should be segregated into human based and technology based components (Cheung, 2012). One of the biggest computer based social engineering techniques is Phishing. Social engineers usually send an email with link which requires registration and asking to create a username and password. For ease remembering, people have the same password for all their internet accounts. So it is necessary to consider that people always have to create unique passwords for work accounts different from other outside personal accounts and keep changing it often. Phishing attacks are typically executed through the internet which facilitates mass distribution of emails in a short time frame. In recent times, phishing activities have continued to thrive in spite of the technological measures put in place by organizations, campaign by the target industry sectors and the advent of anti-phishing organizations (Odaro and Sanders, 2010). By specially crafted emails from falsely website the recipients most likely give personal information. The possible indicators in the message, that pointing to phishing, could be misspelling, poor grammar, request for immediate reaction and a lot of inconsistencies in the message.

When we talk of social engineering attacks, the first thought is that is a corporation’s competitions. The corporations mutually want to steal business secrets and confidential information. But don’t forget that the military has secrets to, even in some direction more valuable that could damage the security of the entire nation. To learn military secrets, tactics, and plans is an advantage. Social engineering attacks framework is seems to be very huge. On the web site SECURITY THROUGH EDUCATION there are many examples that illustrate how influence tactics were implemented to carry out the social engineering attacks*:*

- *In January 2017 the Israeli Defense Forces published a blog on their website describing an attack on their soldiers and it’s all about the influence tactic known as liking. The attackers (reportedly Hamas operatives) created fake Facebook profiles of attractive young women with the goal of enticing Israeli Defense Forces (IDF) soldiers to befriend them. After building trust and rapport through messaging and photo sharing the operative inquires if the soldier would like to video chat. To do so, requires installing an app that is* *actually a virus. Once installed the soldiers' mobile device becomes an open book. Contacts, location, apps, pictures, and files are all now accessible to Hamas operatives.*

- *The 2016 US presidential election will be remembered, among other things, for spear phishing attacks that targeted high profile members of government. On March 19, 2016, Hillary Clinton's campaign chairman John Podesta, received an alarming email that appeared to come from Google informing him that someone had used his password to try to access his Google account. The phishing email included a link to a spoofed Google webpage informing him to change his password. Mr. Podesta clicked the link and changed his password, or so he thought. Instead, he gave his Google password to Fancy Bear, a Russian state-sponsored cyber espionage group.*

Spear phishing can be much harder to spot, because it appears to come from a trusted source and include information specific to the recipient. The trouble is that a social engineer only needs to fool one person in your organisation to gain access to your networks and data (Winder, 2018). So, who is the security weakest link? The conviction that the people are the weakest link is completely justified.

Mitigation of social engineering appears and influence

Unfortunately, humans can often be a hindrance to cyber security that really concern. The best security system can be punctured by poor staff practices causing catastrophic consequences. Social engineering mitigation is not as easy as ensuring hardware security (Hadnagy, 2011). Hadnagy (2011) highlights the fact that with traditional defensive security the organizations throw money into intrusion detection systems, firewalls, antivirus programs, and other solutions to maintain perimeter security. But, with social engineering no software systems exist that can attach to employees to remain secure. Additionally most of the organizations believe that they are safe, surrounded by their "fence" until one day, when somebody from outside make a hole on the "fence". Suddenly, the perspective shifts and weaknesses float. Samani and McFarland (2014:17-18) highlights three categories of control that can be used to mitigate the risk of social engineering. They are: people, process, and technology. The controls, according to Samani and McFarland are not exhaustive, and may not be applicable to all organizations. They are as follows:

People:

- **Provide clear boundaries:** All staff should be keenly aware of the policies regarding the release of information and have clear escalation paths should a request fall outside of their boundaries.

- **Ongoing education:** Implement a security awareness program to consistently educate employees over time. Use tools such as the McAfee Phishing Quiz to highlight specific tactics commonly used in attacks.
- **Permission to verify:** Provide staff with the confidence to challenge even seemingly innocuous requests. An example of this is to challenge people when attempting to tailgate into offices.
- **Teach the importance of information:** Even seemingly innocuous information such as telephone numbers (enabling information) can be used to stage an attack.
- **Create a no-blame culture:** The targets of social engineers are victims. Punishing specific employees who have been deceived will make all staff less likely to admit to releasing information. Once conned, they could come under the control of the social engineer, who can then use blackmail.

Process:

- **Bogus call reports:** When a suspicious activity has occurred, staff should complete a report that details the interaction. This assists investigations.
- **Informative block pages:** When employees reach a malicious web page, use a block page to inform them why they cannot proceed. This will cause them to reflect on their prior action and can help identify sources of attack.
- **Customer notification:** When callers are denied information, the organization should notify them and verify whether the caller was entitled to the information. Organizations should also consider how they communicate with customers. For example, PayPal includes guidance for users that helps identify if emails they receive are genuine: “A real email from us will never ask for your bank account number, debit, or credit card number etc. Also we’ll never ask for your full name, your account password, or the answers to your PayPal security questions in an email.”
- **Escalation route:** A clear reporting line for front-line staff to escalate any doubts they may have about interacting with potentially fraudulent messages.
- **Tiger testing:** Routinely test staff for their susceptibility to social engineering attacks over the use of multiple communication channels. This provides a tool to measure the effectiveness of training programs.

Technology:

- **Call recording:** Routinely record incoming telephone calls (while following federal and state wiretapping laws) to assist investigations.
- **Bogus lines:** Route calls that are believed to be suspicious to a monitored number.

- **Email filtering:** Remove fraudulent emails containing known and never-before seen malware.
- **Web filtering:** Block access to malicious websites and detect malware inline with access to the Internet.
- **Strong authentication:** Although leveraging multifactor authentication will not eliminate the risk of users being socially engineered into giving up their authentication credentials, it will make the task more difficult for would-be attackers.

Good security policies and procedures cannot be effective unless they have been consistently applied by the employees. They contain standards and guidelines in order to mitigate the risks of social engineering attacks. These policies are even more significant when it comes to preventing and detecting social engineering attacks (Mitnick and Simon, 2002). On the other hand as Mitnick and Simon (2002) state, it is important to note that security policies do not last forever. As business needs change, as new security technologies come to market, and as security vulnerabilities evolve, the policies need to be modified or supplemented.

Knowledge is power, it is true. In this sense, education is the best defense against most social engineering attacks (Hadnagy, 2011). Protection against social engineering attacks always starts with education and training. The education and training programs should cover the all safety procedures, policies and methods in order to raise awareness of possible attacks by social engineering. To develop a successful training program, you have to understand why people are vulnerable to attacks in the first place.

The education for prevention to become a victim of the social engineering should be focused to the employee to: slow down, research the facts, delete any request for financial information or passwords, beware of any download, reject requests for help or offers of help, set spam filters to high, don’t let a link in control, know that foreign offers are fake, secure computing devices. On the other hand, Hadnagy (2011) thinks that security through education cannot be a simple catch phrase, it has to become a mission statement.

According to Mitnick and Simon (2002) the only truly effective way to mitigate the threat of social engineering is through the use of security technologies combined with security policies that set ground rules for employee behaviour, and appropriate education and training for employees. Employees have to know that a click on suspicious links might unguarded their log-in credentials and company confidential information. In other words as Mitnick and Simon (2002) say a security training program requires substantial support and the training effort needs to reach every person who has access to sensitive information or corporate computer systems. It must be on-going process, and must be continuously revised to update personnel on new threats and vulnerabilities.

Conclusion

The human "disease to please" and lack of ability to say "no" are more frequently abused in everyday life. Social engineering has significantly influenced cyber security and it may be only a matter of time until a social engineer targets employees at your organization. The doctors, psychologists, and therapists often use manipulations in order for their patients to take actions that are good for them. On the other hand, manipulation and persuasion in all their forms are also much used by social engineers. In fact it is easier to find a patch for a technical problem than a patch for human stupidity.

The solution of the problem still doesn't exist. Internet has possibility to facilitate mass distribution of emails and the social engineers widely use that, so it is important to understand what indicates that it is a fraud. Also, understanding categories of controls (people, process, and technology) that are used to mitigate the risk of social engineering is very important issue. Security technologies combined with security policies are very important for the security of the organizations and combined with proper education it is the appropriate way of social engineering mitigation.

New threats and vulnerabilities are always around us, so the concern deriving from social engineering is not a "destination by itself", it is a "journey" with no end.

References

1. Cheung, A. (2012) Social Engineering, ACC 626 Spring 2012, http://mirror.thelifeofkenneth.com/sites/qt.vidyagam.es/library/Social%20Engineering/Social%20Engineering%20-%20Alvin%20Cheung.pdf
2. Evans, J. N. (2009) Information technology social engineering: an academic definition and study of social engineering – Analyzing the human firewall, Graduate Theses and Dissertations, Iowa State University. http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1701&context=etd
3. Hadnagy, C. (2011) Social Engineering: The Art of Human Hacking, Indianapolis:Wiley. http://sin.thecthulhu.com/library/security/social_engineering/The_Art_of_Human_Hacking.pdf
4. Lord, N. (2019) Social Engineering Attacks: Common Techniques & How to Prevent an Attack- PANEL OF DATA SECURITY EXPERTS, DATA INSAIDER, DIGITAL GUARDIAN, January 14, 2019. https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

5. Mitnick, D. K. and Simon, L. W. (2002) The Art of Deception: Controlling the Human Element of Security, Indianapolis: Wiley. http://sbisc.ut.ac.ir/wp-content/uploads/2015/10/mitnick.pdf
6. Odaro, S. U. and Sanders, G. B (2010) Social Engineering: Phishing for a Solution, Centre for Security, Communications & Network Research University of Plymouth, U.K. https://pdfs.semanticscholar.org/02fe/f8cd17d891ddb66b8e6d6cc5b193af898b5e.pdf
7. Peltier, R. T. (2012) Social Engineering: Concepts and Solutions, 20 June 2012. http://www.infosectoday.com/Norwich/GI532/Social_Engineering.htm
8. Samani, R. and McFarland, C. (2014) 'Hacking the Human Operating System: The role of social engineering within cybersecurity', Report, European Cybercrime Centre (EC3), Intel Security. http://www.mcafee.com/de/resources/reports/rp-hacking-human-os.pdf
9. SECURITY THROUGH EDUCATION, The Social Engineering Framework, Social engineering tools, Spying or Espionage. https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/spies-espionage/
10. Shen, W. (n.d) Active Social Engineering Defense (ASED), Defense Advanced Research Projects Agency. https://www.darpa.mil/program/active-social-engineering-defense
11. Winder, D. (2018) 'Social engineering: the biggest security risk to your business', IT Analysis. Business Insight, ITPRO, 23 Maj 2018. http://www.itpro.co.uk/social-engineering/30017/social-engineering-the-biggest-security-risk-to-your-business