2016 IEEE 4th International Conference on Future Internet of Things and Cloud

Social Engineering Attack Strategies and Defence Approaches

Ibrahim Ghafir
FI, Masaryk University
School of Computing, Manchester Metropolitan University
ghafir@mail.muni.cz

Vaclav Prenosil
Faculty of Informatics
Masaryk University
Brno, Czech Republic
prenosil@fi.muni.cz

Ahmad Alhejailan
School of Computing, Manchester Metropolitan University
Manchester, UK
14056704@stu.mmu.ac.uk

Mohammad Hammoudeh
School of Computing, Manchester Metropolitan University
Manchester, UK
M.Hammoudeh@mmu.ac.uk

***Abstract*—This paper examines the role and value of information security awareness efforts in defending against social engineering attacks. It categories the different social engineering threats and tactics used in targeting employees and the approaches to defend against such attacks. While we review these techniques, we attempt to develop a thorough understanding of human security threats, with a suitable balance between structured improvements to defend human weaknesses, and efficiently focused security training and awareness building. Finally, the paper shows that a multi-layered shield can mitigate various security risks and minimize the damage to systems and data.**

***Keywords*—Social Engineering, Security Awareness, Cyber security.**

I. Introduction

The frequency and costs of cyber security incidents continue to rise making it extremely challenging to defend against today's attacks. To provide security, various system components require adequate security measures to guarantee reasonable or maximum protection of the complete system. According to [1], this can be achieved via implementing two levels of security: technical security and administrative security. Technical security is further classified into IT security, involving computer and communication security, and physical security. All these security levels are aimed at safeguarding systems against possible intruders and malicious criminals.

Aspiring intruders usually possess three key qualities that enhance their ability to penetrate secured systems. These are: method, which entails having the requisite tools, skills and resources to carry out the attack; opportunity, which involves access and time for the intruder to perform the attack; and motive, which is the core reason to execute the attack. With the resources available online, system knowledge can be easily acquired with varied attack modes. This, coupled with a motivation (such as for financial reasons, corporate espionage, data stealing, among others) and time can result in successful attacks on the targeted system. One particular technique that has had devastating effects is social engineering.

There is a consensus in the research community that humans are your weakest link in an information system. Exploiting human vulnerabilities using phishing techniques rather than technical ones is becoming the major threat to the security of information systems. This paper provides the readers with an overview of social engineering and addresses the issue of human vulnerabilities. It defines and classifies social engineering attack techniques and strategies. It also presents the current defences approaches against such attacks to mitigate the risks and minimize the damage to the systems and data.

The remainder of this paper is organized as follows. Section II defines social engineering attack. Social engineering techniques are classified based on the employed attack strategy in Section III. Section IV shows the current defences approaches against social engineering. Section V concludes the paper.

II. What is Social Engineering?

According to a report published by the Centre for the Protection of National Infrastructure [2], social engineering has been defined based on psychological and security terms by various organizations and people. In [3], it is defined as "breaking an organization's security by interactions with people". Another individual, Kevin Mitnick (a hacker once listed by the FBI as most-wanted), describes it as "taking advantage of people's naivety via influence, persuasion and manipulation to obtain vital information" [4]. It is further described as a skill set utilized by an unknown individual to obtain trust and access to an organization via someone in the organization and consequently guides them to alter IT system rights or access that ultimately grants the individual access rights [1]. In a nutshell, social engineering can be defined as a breach of organizational security via interaction with people to trick them into breaking normal security procedures.

Social engineering basically entails exploitation of people's common sense to acquire vital or critical company information (such as user IDs, passwords, or corporate directories) from unsuspecting employees. For instance, this can be through convincing an individual, through trickery, to hand over a password. This technique is usually used by hackers where technical means have failed to penetrate a target system. As such, it specifically targets human psychology and the natural need for being helpful. In terms of the business environment, most companies have installed high-tech defense systems, such as firewalls, internet server hardening and even use of secure internal file transfers, to guard their systems and networks against unauthorized entry, while overlooking the social aspects. It is emerging that the biggest risk to information security in an organization is not technology-related, rather it is in the inaction or action of employees and other organisational personnel that consequently leads to security incidences. For

978-1-5090-4052-0/16 $31.00 © 2016 IEEE
DOI 10.1109/FiCloud.2016.28

instance, an employee may disclose vital information regarding business systems, e.g. the name of the organisation's security platform, on social media that could be used by malicious attackers for social engineering attacks. In some occasions, an employee may choose to ignore and not report unusual activity (related to information breach), or he could gain access to sensitive information beyond the user's role and credentials through unethical means. All these scenarios expose the organisation to security risks with the mishandling of crucial and sensitive information. Social engineering is also considered as the most common technique used in Advanced Persistent Threat (APT) attacks [5].

III. Social Engineering Attack Strategies

A vast number of social engineering attacks exist to acquire information or access systems through exploiting unsuspecting employees. Despite the varied modes, the attacks do follow a typical cycle. These are [6]:

1) Information gathering
2) Development of relationship
3) Exploitation of relationship
4) Execution aimed at objective achievement

The information gathering process can be obtained from public sources such as web pages, social media posts, phone books, jobs portals, amongst others, or from a previous social engineering attacks. The information from this step is utilised in developing a mutual relationship with targeted persons. In step 2, relationship development is aimed at creating a rapport with the target based on known human tendencies and characteristics of being helpful and trusting. When step 2 is successful, the attacker exploits the target to reveal vital information such as passwords, credit card numbers, login details, secret information, amongst others. This information acquired can either be the ultimate aim of the attack, or the commencement of the next phase. In the last step the attacker tries to achieve the ultimate goal, which may involve iteration of previous steps.

Social engineering techniques can be largely classified into two categories: attacks based on the physical locations (computer-based attack) and attacks based on psychological means (human-based attack).

A. The Physical Locations

Computer-based attacks rely heavily on technology to manipulate and trick a target into submitting information required by the attacker to execute his malicious deeds. For example, the use of a pop-up window notifying a user that their network connection has been lost and are required to re-enter their login details to reconnect. Such information would then be emailed back to the intruder via an installed program on the targeted individuals system. It is effective when an attacker has already had relative system access at a low level. This class of attacks can be effected based on these three physical settings: the workplace, by telephone, or online [7].

1) The Workplace:
Through impersonation (say a consultant, trusted third party or maintenance worker), tailgating, masquerading, or after-hours entry an attacker can easily stroll into an organization or company's main entrance. Once physically inside the premises, the attacker can "shoulder-surf" or eavesdrop passwords, obtain sensitive documents (carelessly left on employee workstations), gather passwords, or penetrate the corporate network (via unguarded network ports). Once the required information has been gathered, the attacker may exit the premises and continue exploiting the network remotely, their convenience [1].

2) By Telephone:

This technique represents one of the most common means utilized by attackers. This is particularly via an organization's help desk. Most attackers prey on organizations' PBX systems or customer care help lines within the aim of appearing like they are calling from within the organization (not from a line outside the organization). This method allows an attacker to be relatively anonymous, and remain so, while obtaining information such additional telephone numbers, sensitive documents, passwords, or any other relevant information to the attacker [8].

3) Online:

This attack-mode is based on several platforms including online instant messaging platforms, E-mails, via social media platforms, etc. This is based on several modes of implementation. For instance, an attacker would want a target to install malicious programs on their local machines, such as worms or viruses. An attacker would trick a target into submitting personal information or passwords through filling out a form, commonly referred to as Pharming or Phishing, via legitimate-looking e-mail requests such as banks from. An attacker would also obtain detailed information via carrying out of web searches related to company information in cases where organisations put up detailed information on their web sites including services, products, staff details, among others that would be used in target acquisition. Another method is via using online curricula vitae through which provide detailed personal information related to a target's place of work and organisational rank to be used in the target acquisition phase [9].

B. The Psychological Methods

The popular and easier SE mode still remains human-based. It heavily relies on deception and interpersonal relations by utilizing specific techniques such as name-dropping, intimidation, belittling, asserting authority, and flattery. It is based on utilization of one-to-one communication between the attacker and the targeted individual. Mostly, this method category heavily relies on carrying out a basic background research, where information acquisition, on the targeted organization, is carried out. Some of the techniques used to gather this information include: shoulder surfing and eavesdropping. Once the basic information acquisition is guaranteed, several methods, as explained in the next section, are used to manipulate the target in order to acquire additional information [10].

1) Authority:

Implications and assertions of authority are a source of effectively gaining vital information from an unsuspecting target, especially a newly recruited employee or a low-level staff member. The most commonly used method involves

an attacker claiming to be from the security department, IT department, manager, or other high-level authority and utilising this perceived position obtaining information related to password resetting or new password through threats or intimidation. For instance, the attacker may threaten to report a staff member to their supervisor for incompetence or intimidate the target staff that they are late in delivering important data or information to the organisation's chief executive. Such acts would see the intimidated or threatened staff member giving out the information as demanded. It is of note that this method is highly effective in hierarchical organization [11].

2) Natural Inclination to Help:

Humans have a natural tendency to assist those who are in need of help. Unfortunately, this aspect is known to social engineers who take advantage of this human nature. For instance, a social engineer may impersonate a deliveryman carrying many boxes into a premises and gain physical access to a target building when an employee decides to hold open the door. In another situation, an attacker can impersonate a desperate employee calling the IT Help Desk for access to the corporate network from home, resulting in the attacker acquiring sensitive information related to company networks [12].

3) Liking and Similarity:

By carrying out casual conversation, an attacker can gain insights on a target aimed at developing persona connections. For instance, sharing similar activities and hobbies, support for the same sports team, or claiming to birth roots or area. There is a natural tendency for humans to associate with individuals of similar interests or origins. In the process, the attacker is able to establish a rapport making it easier to acquire sensitive information from the target as they trust them.

4) Commitment and Consistency:

Attackers also exploit employees' nature of wanting to be seen as trustworthy and committed to execute their attacks. For example, an attacker would instruct an employee to execute a certain task warning of dire consequences or reprimand if non-compliance is exhibited. This can be implemented by instructing a new staff member to implement certain security policies and in the process requiring the target to share their credentials aimed at ensuring compliance. This results in the employee sharing their system credentials that the attacker would use to access the organisation's system.

5) Reciprocation:

The norm in social interactions dictates that if an individual gives us something, it will only be courteous to return the favour. This aspect is referred to as reverse social engineering [9]. The technique involves the attacker creating a situation that results in the target encountering a problem, prompting the said target to seek assistance from the attacker, who resolves the situation. In return, the victim offers the attacker requested information, felt as obligated to the attacker.

6) Low Involvement:

This involves the attacker requesting for information or carrying out a task of employees who have little or no interest related to the information or task request. This can include the receptionist, cleaning crew or even the security guard. These targets are seemingly picked by the attacker due to their ignorance and an overwhelming sense of assertion of authority by the attacker, request urgency, and lack of awareness of the consequence. In this method, vital organisational information could fall into the hands of the attacker [13].

IV. Defence Approaches Against Social Engineering Attacks

One aspect that distinctly distinguishes social engineering attacks from technical attacks is the technical level of staff involved in the act. A typical technical attack would involve a given combination of staff from the information security department or the IT department. These targets are highly knowledgeable in the organisation's systems in matters related to security awareness, technical knowledge and ways in which the systems may be attacked. However, social engineering attacks target anyone, from the executives in the organisation to the cleaner who works night shifts. The calibre of employees targeted may lack technical system knowledge nor be aware of the security concerns when in their opinion the information they possess or work with is not regarded as sensitive or classified. Whereas it would be practically impossible to eliminate social engineering breaches, the risks can be mitigated and the damage to systems and data can be minimised. A multi-layered approach is essential in building a good defence against social engineering attacks to create a large barrier between the attacker and the actual access to the system. For instance, if the attacker penetrates level one, the other levels would ultimately stop him/her from accessing the system. Some of these levels already being implemented include: foundational level, which involves developing a security policy around social engineering; fortress level, which involves resistance training for employees at key installations; persistence level, which involves carrying out ongoing reminders; the offensive level, which entails responding to incidences; and the gotcha level, which involves developing SELM (Social Engineering Land Mines) [1].

A. Improved Physical Security

This forms the basis for implementing a strong social engineering defence by ensuring valuable and sensitive information stays within the organisation. Although it can be easily exploited, especially if the attackers are working from within the organisation, improvement of physical security can be a major deterrent to outside attackers against just gaining physical access and acquiring any information that they may require.

B. Stronger Security Policy (Foundational Level)

Security policies have a specified life span that ideally requires a review date and most importantly maintained in a current state. To achieve this, policies should be reviewed regularly and on a rotational basis, with at least 20% of these policies altered yearly and the entire system in a 5-year cycle. In case of more volatile policies, these should be reviewed more frequently. Some of the policies that can be implemented to guard against social engineering attacks include matters related to: information release, access approval, password changes, modems, help desk, employee ID, shredding confidential documents, etc. On information release,

the policy should have clear guidelines on the personnel and circumstances under which information can be released to the public. For example, all organisational surveys would be designated to a specific employee. Access approval matters related to the policy should include: signing of security agreement prior to granting access, authority and type of access to the system that various employees wield, have a clear guideline on account creation and termination methods, and have defined account creation procedures to ensure elimination of mistakes and confusion.

In terms of password changes, the policy should require a strong combination of characters, including lower, upper, special, and numbers while also setting out the frequency of password changes. On edge devices, a good policy will prohibit use of such devices on the organisation's intranet since they would bypass company firewalls, creating an open door. There can be an audit in place by the IT staff to verify that such devices are not being installed. The help desk should have a clear policy related to giving out information and passwords. A good policy would require verification of the employee based on a number of laid out procedures. In terms of the employee ID, an organisation may develop a policy used in identification of all the organisation's staff (e.g. by wearing an ID tag with a picture of the employee). In addition, visitors would be required to register and assign a temporary ID tag that should be worn. Anyone not complying with these requirements should be reported. Finally, there should be a shredding policy that affects all sensitive documents to avoid the use of the "dumpster diving" technique. Violations of any of the security policies should have a clear and well-known procedure that employees can follow to report failures to comply incidents. Moreover, there should be life cycle policies related to the information system life cycle. This entails storage and destruction of both hardware and data that is no longer required by the organisation [14].

C. Response to Security Infringements (Persistence and Fortress Level)

This involves implementing resistance-training techniques for key personnel, carrying out ongoing reminders, and punishing staff who continuously break policy controls. Resistance-training techniques are aimed at making employees resilient against persuasion techniques that a social engineer may employ. These may include: inoculation, which involves furnishing the organisation's employees with possible weakened arguments a social engineer may attempt to use along with rebuttal argument responses the staff member may use; Forewarning, which entails warning of employees on the possible content of upcoming messages that may come from attackers who will use insincere, deceptive, and manipulative language aimed at stealing information; and Reality check, which encompasses demonstrating the realities of security threats by social engineers to employees by actually demonstrating a social engineering attack on them to show their vulnerability [15].

Carrying out ongoing reminders is a necessity of security consciousness. The ability of employees to resist attempts by a social engineer can only be realised within a short time frame. Creative and regular reminders are mandatory to ensure the staff are aware of any lurking dangers from conversations via email, instant messaging, social media or even phone calls. A good example is an illustration of recent social engineering attempts to the employees that may have been successful or were thwarted. This would ensure that employees are reminded of attacker attempts at any given time making them cautious in their interactions with outsiders.

D. Incidence Handling Procedures (Offensive Level and Gotcha level)

Besides having knowledge on when social engineering attacks may take place, it is equally important to have requisite knowledge on what actions to take in the course of an attack. The two techniques that can be used in such situations are: laying of Social Engineering Land Mines (SELMs) and Incidence response. SELMs refers to system traps laid to stop or expose an attack. As the name suggests, they are usually set to "explode", by surprise, in an attacker's face. In the process, it exposes the attack's secrecy, cripple the process and eventually stop the attack. In addition, SELM will notify the victim's system and the victim of the attempt to enable additional security measures to be implemented immediately. Some of the techniques applied include: a Justified Know-it-all, who represents a person well versed with all employees in a department and can easily identify an intruder and quickly implement security mechanisms in case one is spotted; centralised security log, which involves logging and monitoring of all security events in a central file and where irregular patterns can be easily identified and relevant employees warned of impending attack; having a Call Back policy, which would require system administrators and Help desk personnel calling back any employees requesting for questionable information or password reset aimed at verifying the true identity of the caller; Key questions, which encompasses having a number of questions asked to anyone requesting for password resets or internal information to verify their identity (an example is the 3 Questions Rule); and the "Please Hold" policy, which involves putting on hold any suspicious requests for purposes of seeking additional information from other sources related to the request prior to responding, to ensure it is legitimate, or requires further verification, or should be denied entirely [16].

V. Discussion and Future Work

Social Engineering attacks are serious threat to information security. They are exploited to acquire information or system access from unsuspecting employees. This paper has presented a background on social engineering attack, classified social engineering techniques and strategies and reviewed the current defence approaches against such attacks.

Based on recent large scale social engineering attacks, it is evident that addressing human security weaknesses is not high on the targeted companies agendas. Even now, most employees outside the IT department believe that information security is an IT issue. This work advocates information security is not the responsibility of a single user, instead, it is the responsibility of all users associated with an organisation, from the cleaning team to the sales representatives, admin staff to security managers. It is vital to educate employees about cyber security issues and threats. Security awareness is a powerful instrument in the battle against cybercrime. In reality the distinction between personal life and work life can become convoluted, for example the concept of BYOD (bring your own

device). If a user shares personal information on social media, this could pose a threat to the company of the user. Social engineering attacks can use this personal information against an organisation.

In the current financial climate, companies have cut their training budgets and investment in IT security solutions to record levels. This motivates our future work to develop a security awareness program aiming to achieve two related objectives: awareness, whose aim is to raise the collective importance of security controls and security as a whole; and training, is aimed at facilitating increased in-depth understanding by the system user. Because finding a portion of the training budget to deal with human security can be a real challenge, the desired training program will employ context aware self-learning approach that allows individuals to learn about the security risks related to the task currently at hand. Such an approach will save companies a fortune on expensive training programs and will give employees the ability to learn by example. This method particularly suits the non-technical audience.

REFERENCES

[1] M. I. Mann, *Hacking the human: social engineering techniques and security countermeasures*. Gower Publishing, Ltd., 2012.

[2] CPNI, "Social engineering: Understanding the threat," http://www.cpni.gov.uk/documents/publications/2013/2013065-social-engineering.pdf?epslanguage=en-gb, accessed: 25-3-2016.

[3] M. Bezuidenhout, F. Mouton, and H. S. Venter, "Social engineering attack detection model: Seadm," in *Information Security for South Africa (ISSA), 2010*. IEEE, 2010, pp. 1–8.

[4] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2011.

[5] I. Ghafir and V. Prenosil, "Proposed approach for targeted attacks detection," in *Advanced Computer and Communication Engineering Technology*. Springer, 2016, pp. 73–80.

[6] A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: Affect-based model," in *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for*. IEEE, 2013, pp. 508–515.

[7] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technology in Society*, vol. 32, no. 3, pp. 183–196, 2010.

[8] J.-W. Bullee, L. Montoya, M. Junger, and P. Hartel, "Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention," 2016.

[9] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu, "Reverse social engineering attacks in online social networks," in *Detection of intrusions and malware, and vulnerability assessment*. Springer, 2011, pp. 55–74.

[10] J. Long, *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. Syngress, 2011.

[11] F. Mouton, L. Leenen, and H. Venter, "Social engineering attack examples, templates and scenarios," *Computers & Security*, 2016.

[12] J. Goodchild, "Social engineering: The basics," *CSO Online*, 2012.

[13] D. Kvedar, M. Nettis, and S. P. Fulton, "The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition," *Journal of Computing Sciences in Colleges*, vol. 26, no. 2, pp. 80–87, 2010.

[14] S. Satish, "Educating computer users concerning social engineering security threats," Feb. 10 2015, uS Patent 8,955,109.

[15] X. R. Luo, R. Brody, A. Seazzu, and S. Burd, "Social engineering: The neglected human factor for," *Managing Information Resources and Technology: Emerging Applications and Theories: Emerging Applications and Theories*, p. 151, 2013.

[16] K. Beckers, L. Krautsevich, and A. Yautsiukhin, "Using attack graphs to analyze social engineering threats," *International Journal of Secure Software Engineering (IJSSE)*, vol. 6, no. 2, pp. 47–69, 2015.