The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.43 e-ISSN: 2251-7545

Impact of Social Engineering on knowledge Community

Bassant M. Abagouri
Faculty of Computer and Information science, Ain Shams University, Cairo, Egypt
bassantai@yahoo.com

Ibrahiem M. M. El Emary
King Abdulaziz University, Jeddah, Saudi Arabia
omary57@hotmail.com

Bader A. Alyoubi
King Abdulaziz University, Jeddah, Saudi Arabia

Abstract ***—Social engineering and offensive security, adequate attention should be paid because of their ability to take advantage of the weakness of human trust and show. Social engineering attack can successfully lead to other serious crimes such as identity theft and industrial espionage. This is not only at the organizational level, but also at the individual level. This paper aims to examine some details regarding social engineering attack against an organization with their permission. The paper concludes important recommendations to reduce the threat of social engineering as well as the main architect of social attention; care should be taken to avoid the problems faced by various organizations.***

Keywords— ***Information Systems, Attack, Social Engineering, Security and Community***

I. INTRODUCTION

One many challenges facing developers during the development of modern information systems (IS) is the security strategy and policy used to protect such systems. It is mainly engineering information systems security with protection means cost-effective and operationally effective information systems of unwanted events [1,2] and also claims security engineering on building systems to remain dependable in the face of malice, fault or bad luck. Therefore, to design an effective security system it is important to know what potential threats, so that we can take appropriate measures to combat. However, no matter how good and protection, and the attackers as possible (until now) have the potential to expose the weaknesses of the system. In addition, during the analysis and design for developers, most of the time, we suppose that infrastructure is 100% trustworthy. But this may not be the case, making the forecast every possible attack during the very difficult system, allowing an attacker to attack on the system with the types of attack that developer cannot determine or signed during development. On the other hand, axiom known computer security states that the only completely secure computer system is not running completely. Social engineering is the name given to a class of security attacks, dealing with other

A.

people to reveal information that could be used to steal data, access to systems, and access to cellular phones, money or even our identity. Such attacks can be very simple or very complex. Access to information over the phone or through the Web sites you visit has added a new dimension to the role of the social engineer [3]. To attack our organization, social engineering hackers exploit the credulity, laziness, good manners, or even enthusiasm of our staff. Therefore it is difficult to defend against socially engineered attack, because the goals may not realize that they were tricked, or may prefer not to admit it to others. Goals of social engineering hacker, someone who attempts to gain unauthorized access to our computer systems similar to those in any other hacker ware. Social engineering hacker is a professional one who attempts to persuade staff to provide information that will enable him or her to use our systems or system resources. Traditionally, this approach is known as a confidence trick. Many medium-sized and small companies believe that hacker attacks are a problem for big companies or organizations that provide great financial rewards. Although this may be the case in the past, and the increase in cyber-crimes means that hackers now target all sectors of society, from corporations to individuals [2]. The criminals stealing directly from the company transfer of funds or resources, but the company can also be used as a starting point from which we can commit crimes against others. This approach makes it difficult for authorities to track down these criminals

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

II. RELATED WORKS

To protect our staff from social engineering attacks, we need to know what kinds of attack to expect, understand what he hacker wants, adjusters may be useful for our organization. With this knowledge, we can increase our security to include social engineering defenses. This paper assumes that we have a security policy that defines the objectives, practices, and procedures that recognize the company necessary to protect information assets, resources, and staff against technological or physical attack [1]. Changes to security policy will help provide staff guidance on how to act when a person or computer application that attempts to compel or persuade them to expose business resources or disclose security information.

Typically, many organizations have information that has value to justify the costly protection mechanisms. Important information may include patient records, and financial statements of companies, electronic funds transfers, and access to financial assets, personal information about customers or employees. The compromise of sensitive information can have serious consequences, including the loss of customers, being criminal cases against corporate executives, civil law cases against the organization, and the loss of money, loss of confidence in the organization, and the collapse of the organization [4]. To respond to threats and information security plans to extend its control over information assets.

Information security plans identify protection mechanisms for information management.

There is usually too much reliance on technical security mechanisms, such as firewalls, user passwords and closed networks, operating system protection mechanisms. There is usually a discussion on the mechanisms of physical protection and other security issues. There seems to be a belief among the profession computer security and information that everyone understands the operational security requirements for information protection. For this reason, most of the funding for the leaked information security technical mechanisms, and little, if any, is assigned to security awareness and operational security training.

Large commercial organizations, confirms that a lot of people with computers do not understand the value of the information they access. Users revealed a variety of sensitive information, including the names of the employees and management cost information, and phone numbers for modems, and customer data [4]. Surprisingly, user IDs and passwords is very easy to obtain. Along with phone numbers of modems and passwords give attackers access to all corporate information when combined with other technical means.

Phishing seeks to trick users into giving up information such as usernames and passwords. Phishers often say an account is about to expire and the victim needs to confirm their account information. Anti-phishing services and toolbars attempt to protect users from phishing attacks. Many users do not understand cues provided by anti- phishing tools or fraudulent websites indicating fake websites. Julie Downs et al recruited 20 people with computer experience, but without any computer security experience. The participants received information regarding a persona they were to portray and to read and react to several emails. Several emails were legitimate whereas the rest contained various forms of phishing attacks [12].

Hacking threat can be for financial gain or personal revenge. Spyware threat can be social or personal. Virus threat can be economical. Bitnet and Trojan ware threat leads to social and national security. There are various types of threats

- Personal Threat / Organizational Threat
- National Security Threat
- Economical Threat

Most Parasites writer or phishers have their main purpose as Money and hence most of the time it is related to banking. Brand attacked in November 2009 were banking, ecommerce, IT services and other. There were 29 countries whose brands were attacked. During November 2009, In China, the ecommerce sector remains a primary target. Due the 2010 FIFA World cup, Phishers are launching attacks masquerading World cup related sites. From the above report you can see that most of the time phishers are attacking banking system [13]. The traditional attack cycle is shown in Fig.1. Another possibility is to view this from the point of a social engineering attack cycle, which consists of four different phases (see Fig. 1) [14]. First phase entails gathering of background information, which enables the attackers to better succeed in developing relationships with their targets. Once this position of trust is achieved, it is exploited by getting the target to reveal information or perform actions. When the target has completed the task, the execution of the attack cycle is complete and the attacker has achieved his goal. This can be followed by yet another cycle to gain further privileges or information as it is less conspicuous,

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

if the attacker only tries to achieve small objectives at the time and with the same victim. In essence, the separate requests to different people can seem innocuous enough to each individual, but the combined results can have a powerful effect.

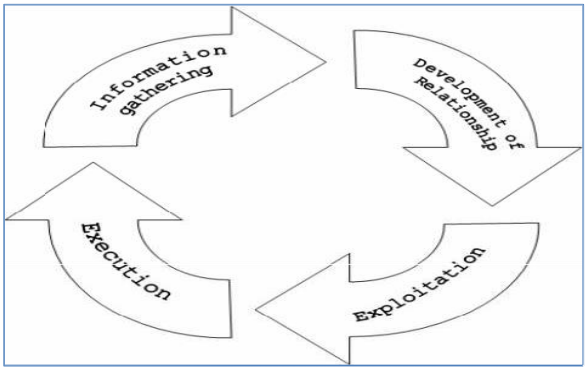

Fig. 1. Social engineering attack cycle [14]

III. THE MAIN NTAILS OF SOCIAL ENGINEERING

Since social engineering attack non-functional weaknesses in the area of security, there must be discussion of what are the weaknesses in the area of security. Basically, there are two types of vulnerabilities that allow social engineering to occur. Surely, the lack of security awareness facilitates social engineering attacks. In other words, people do not know how to respond appropriately to violations [5]. Plans and procedures to facilitate the poor also attack. In many cases, the design plans and procedures to thwart FW would be, but has not been tested by an independent source to determine their adequacy.

A. Human Weaknesses

People will give out the information for several reasons. In most cases, people just want to be helpful, because this is their work and/or nature. People can also be intimidating for the release of information, either by being made to believe that superior wants information or by trying just to make annoying person goes away. Corporate spies and many hackers understand that what is considered a positive attribute profile can easily be exploited and used against the individual.

B. Untested Plans and Procedures

While organizations understand the threats and vulnerabilities, and try to address the weaknesses through appropriate operational procedures, it is difficult to determine whether sufficient action has not been tested. A good example of an untested is relying on internal identifiers [3]. Many organizations create internal ID that is used to authenticate an employee to another employee. For example, many organizations rely on the social security number for identification. It takes very little effort for attackers outside to get a social security number before attempting to get the required information.

Social engineering attack may consist of several small attacks, and that in them may be illogical. Unfortunately, the total social engineering attack is greater than the sum of its parts. Will probably go small attacks unnoticed, can occur over several months. While the Organization has a documented mechanism requires, there must be procedures to protect authentication mechanisms [4]. This is where a large number of security plans fail. Many organizations test a specific part of a security plan or procedure, but must be test plans and security procedures as a whole.

IV. THE POOR SECURITY AWARENESS

Organizational information security plans will address fundamental issues in computer security. These issues could include failure to disclose passwords, not give sensitive data unless we confirm the identity of the caller, and so on, most plans do not include realistic procedures to make staff aware of the security procedures. Many security experts say that the public understood basic security issues, such as the importance of having a password. These issues are considered to be common sense by the computer and security personnel. However, there can be by common sense, there must be common knowledge.

There is very little known when it comes to the relevant computer security issues.

Deploy computer passwords one such case. And a very large percentage of users do not understand the importance of having a password for authentication and access to a computer system [6]. They don't realize that it can be accessed from the account anywhere in the world, given the appropriate access point. Users do not understand the lengths that people will go to get the information that they have access to on a

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

daily basis. Many people do not understand that throw something in the garbage does not mean that the information is destroyed. What is garbage to a user are extremely valuable for hacker, and most people don't understand this concept.

V. VARIOUS AFFECTED ASPECTS OF PSYCHOLOGY IN SOCIAL ENGINEERING

There are three main aspects of social psychology that will help us understand the methods used by social engineers. These include:

- Using alternative methods;
- Attitudes and beliefs that affect human interactions, and
- Techniques of persuasion and influence.

The concept of alternative methods, there are two ways: direct and secondary road. In the direct path of the social engineer was actually just asking target to get information. This doesn't work very often, but it is always worth a try. If that fails it is a systematic approach to getting what they want [7]. Are willing to invest time in the relationship and get false relationship with the intended victim. They are logical arguments that will work for the victim to get them to act.

Secondary roads or indirect social engineer will make potential victims more vulnerable by making some statement at the outset to trigger strong emotion like excitement or fear. The social engineer willing to spend time to get to know mark or it may be a fellow officer, it can be arranged that plays on the background of the victim. In a typical interaction our attitudes and beliefs about the request to start service basic idea that each party is who they say they are. The interaction of social engineering, but the victim retains this idea. Effective social engineer depends on knowledge that the victim will rarely question who they are.

VI. MAIN ADVICES THAT SHOULD BE CARE

This item related to the strong security measures and very successful attackers in a very short period of time. While the attack may seem very long and complex time, in less than three days, and cost very little. Many of the vulnerabilities exploited by attackers are common for most companies [6]. These weaknesses will expand to help businesses overcome many weaknesses exploited by social engineers.

A. DO NOT RELY UPON COMMON INTERNAL IDENTIFIERS

Sometimes called the attackers themselves to authenticate as genuine by providing their Ernployee. Fortunately for the attackers, officer numbers are usually used and can be easily obtained from real employees [8]. The attackers on a list of numbers, and they were ready to meet any challenge. Many companies rely on similar IDs. Should companies have separate ID to support its activities? A separate ID on relevant activities separate computer support staff posts and provide additional security for both employees and computer activities.

B. IMPLEMENT A CALL BACK PROCEDURE WHEN DISCLOSING PROTECTED INFORMATION

It is possible that many attacks if employees check caller ID by contacting them again in the correct phone number, as it appears in the phone book company. This procedure creates a minimum inconvenience legitimate activities, but compared with the scale of potential losses, justified the inconvenience. If there is a need to connect again anyone seeking personal information or private would be less concessions of all complexions. Caller ID services may be acceptable for this purpose.

C. IMPLEMENT A SECURITY AWARENESS PROGRAM

While giving your password to a stranger may seem silly to the reader of this paper, it seems harmless to many computer users. Companies spend millions of dollars to get the status of your hardware and software security devices, but are ignoring the public awareness program [8]. Computer professionals cannot assume that basic security practices are essential for the non-specialist computer. You can perform A security awareness for good program possible cost and can save millions of dollars in company losses.

D. IDENTIFY DIRECT COMPUTER SUPPORT ANALYSTS

Every company employee is familiar personally with the computer analyst. There must be one analyst for a term of not more than 60 users [9]. Analysts should be the focal point of all computer support, and should be the only people to communicate directly to users. Users should be instructed to immediately contact their analyst, if contacted by someone claiming to be from computer support.

E. CREATE A SECURITY ALERT SYSTEM

During the attacks, he realized that the attackers even if it is detected, there doesn't seem to be a way for the

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

employee to alert other staff from possible attack. This shows that even if there was a compromise in the attack, the attack can continue with minimal changes. Basically, to improve compromise attack, because the attacker had learned what doesn't work.

F. Social Engineering to Test Security Policies

Social engineering is the only conceivable method to test security policies and their effectiveness. While many security assessments test physical weaknesses and vulnerability analyses, a few inherent weaknesses in the human users. It should be noted that only qualified persons and trustworthy should lead the attacks. The attack was done above by trained people within American intelligence agencies were aware of computer security measures and countermeasures.

VII. ROLE OF SOCIAL ENGINEER IN KNOWLEDGE COMMUNITY

The aim of the social engineer to trick someone into giving them what they want [10]. The social engineer preys qualities of human nature, such as:

- Desire to be helpful. We train our staff too. Make sure the customer is satisfied.

The best way to assess the good has a good response from those in need of assistance. Most employees want to be useful, and this can lead to a lot of information.

- There is a tendency to trust people. Human nature is to trust in the fact others even proved that they are not reliable. If someone says they use a certain person, we accept this statement. We must train our staff to obtain independent evidence.
- Fear of falling into trouble. Too many of us have experienced a negative reaction by the heads of the verification of the identity of long or that offend some. The Department must support all employees are assigned and the protection of sources of information for

What scares most companies from social engineers is that the successful social engineer

really is that they receive what they are looking for without raising any suspicion. It's bad social engineers that we know about, not good ones. There are skilled social engineer often attempt to exploit this vulnerability before spending time and effort on other methods to crack passwords or access to systems [10]. Why go to the trouble of installing a sniffer on the network, when a simple phone call to the employee may gain user ID and password required.

A while back a client asked us to see if we could obtain employee access accounts and passwords. They have an aggressive awareness campaign to remind employees of the need to keep the passwords from being compromised. The client wanted to know if we were going to install a sniffer, we told them that we had a better method, we would call his employees. We called twelve employees and had nine people answer our call. We told them we were from network administration and that we needed them to logon so we could troubleshoot a problem. We told them we needed their account identification and password so that our scope could see when they entered the network. Of the nine who answered, eight gave us the information we wanted [11]. The ninth couldn't find the Post- it note that had his password. Social engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone. A successful defense will require an effective information security architecture starting with policies and standards and following through with a vulnerability assessment process.

VIII. CONCLUDED REMARKS AND FUTURE WORKS

After presenting this paper we can ask our self an important question as: Can even the best technical mechanisms have prevented the attack? Only can reduce the use of the word mechanisrns for once the effects of social engineering attacks. Exploit attacker's poor security awareness, information and operational security perspective. Even if the attackers were unable to "get" our passwords, it managed to obtain sensitive personal information, and company. Social engineering attacks revealed similar problems in many organizations. However, each attack results in problems that are specific to being examined. It is for this reason that each threat assessment should include comprehensive social engineering effort by qualified and reliable personnel. Security officers must consider the non-technical aspects of computer security along with technical measures. Finally, we conclude that Organizations must fight social engineering attacks by establishing policies and procedures that define roles and responsibilities for all users and not just security personnel. As well as organization must ensure that, these policies and procedure are executed by users properly hence regular training needs to be given on the latest such incidents. Future works with a focus on websites would facilitate a more

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

ACCURATE JUDGMENT IN RELATION TO USERS' ABILITY TO DETERMINE THE LEGITIMACY OF A WEBSITE.

REFERENCES

[1] Tolga MATARACIOGLU and Sevgi OZKAN, "User Awareness Measurement Through Social Engineering", International Journal of Managing Value and Supply Chains (IJMVSC) Vol. 1, No. F, December F010

[2] [F] T. Mataracioglu, "Social Engineering: Attack and Protection Methods", Tubitak

[3] Uekae", Department of Information Systems Security – Course Notes, Oct. F009. [G] K. D. Mitnick and W. L. Simon, The Art of Deception. Wiley Publishing, F00F.

[4] [K] M. B. Arslantas, "Methods Used in Internet Crime", MEB Head Office of Information Technologies. Nov. F00K : http://egitek.meb.gov.tr/EgitekHaber/EgitekHaber/s7H/bQlsQmsuclarQ.htm

[5] T. Mataracioglu, "Analysis of Social Engineering Attacks in Turkey", Journal of National Research Institute of Electronics and Cryptology (UEKAE), p. 88-9H, Vol. F, No. K, F01

[6] [I] M. Hasan, N. Prajapati, S. Vohara, "Case Study on Social Engineering Techniques for Persuasion", International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks, Vol. F, No. F, Jun. F010.

[7] Fagoyinbo, I. S. Akinbo, R. Y. Ajibode, I. A., Analysis of the Awareness and Safeguarding Against Social Engineering: A Case Study of Federal Polytechnic Ilaro, Journal of Educational and Social Research Vol. 1 (F) September F011

[8] Lemos, Robert : Survey: Identity Theft Hits Three Percent. Security Focus, F00I.

[9] Grander Sarah: Social Engineering Reloaded: Security Focus, F00I

[10] Samuel T. C. Thompson, Helping the Hacker? Library Information, Security, and Social Engineering, Information Technology and Libraries, December F00I

[11] Dimensional Research, " The Risk of Social Engineering on Information

Security: A Survey of IT Professionals. September F011

[1F] Whitman M.E. Enemy at the gate: Threats to Information Security. Communications of the ACM, Volume KI, Issue 8, F00G.

[1G] Schneier B. Secret and Lies. Wiley Computer Publishing, F000.

[1K] Justino E., Oliveira L.S., Freitas C. Reconstructing shredded documents through feature matching. Forensic Science International Volume 1I0, Issues F-G, F00I.