SOCIAL ENGINEERING AND ITS IMPACT ON IT SECURITY IN THE AIRLINE

Karin Hernández – Jozef Galanda

Article acquaints the reader with the social engineering, the individual methods that use social engineers, the active protection against it as the design and implementation in course in LMS Moodle on Faculty of Aeronautics, Technical University of Kosice to support e-learning. At present created course is possible to use as a base for an easier and faster way to obtain information about social engineering. The resulting course can be used not only for the Faculty of Aeronautics but also to other university faculties that use Moodle.

Keywords: Moodle, social engineering, protection, electronic course

1 INTRODUCTION

Currently, there are increasingly talking about identity theft and social engineering, which is dangerous for the reason that users can very easily fooled, and they not even know. This may include different groups of people, but mostly social engineers focus on individuals and generally those less prudent. But the worst is when the social engineer focuses on employee of greater organization to release information that could be harmful. Airlines of the daily use of ICT. They are in constant contact with customers, visitors, competitors. That's the reason why they become more likely to be victims. The objective of our effort was to analyze the various social engineering methods and propose security capabilities of information technology in the airline company against this threat and based on the recommendations of knowledge to create interactive course in Moodle Faculty of Aeronautics for preventing social engineering.

2. SOCIAL ENGINEERING

Social engineering is an art that goes back as far as human history can recall. Is the use of nontechnical means to gain unauthorized access to information or computer systems. In the language of attacker who use social engineering is non-technical social engineering hack. It is the use of tricks, persuasion, personification, emotional manipulation and abuse of trust to obtain information or access to the computer system over a man, with all its weaknesses [1].

2.1 Human-based social engineering

All of these methods are focused on the man, his weaknesses, that the social engineer can use. The social engineer can pretend to be someone else. Often in this method can be used names of senior people in the organization. Social engineers can enter individually into the building and pretend to be employees, visitors or service personnel. Dumpster diving and shoulder surfing can translated as searching through garbage and spying arm. In these examples, the social engineers try to obtain from their victims personal information or password or PIN [5].

2.2 Technology-based social engineering

In these methods the social engineer uses computer that can create executable files and programs through which obtains the necessary information concerning the user or company. The aim is to install malware (malicious file) to a personal computer [5].

2.3 Identity theft as a method of SE

Identity theft occurs when a thief obtains personal information that can be used to impersonating someone else to secure the benefits, obtain goods or services on behalf of that person. Identity theft can have serious consequences for the person whose identity has been stolen, if the victim is required to pay the bills. As well as victims, as well as companies, institutions and individuals who are duped or robbed of identity, may also suffer adverse consequences and losses [5].

2. SOCIAL ENGINEERING METHODS

There are three main methods used by thieves to obtain personal information through the Internet and / or computer. These are:

- ***Malicious software*** **-** is installed on your computer or device (fixed or mobile) and collects personal information about the user during the operations.
- ***Vishing*** - thieves hacked into computers and mobile devices, or otherwise use to obtain personal information of the user.
- ***Phishing*** – thief uses deceptive e-mails that users provide personal information. [1].

Today are equally effective methods of obtaining important information of information systems and information of persons whose identity is essential in carrying out further activities of attacker. Among them we can highlight the following:

Direct application

The social engineer can easily pretend to know nothing about the system and still get the information. This ruse is commonly used when an attacker is able to find sufficient information about the company or find enough information to do the first step. Simple principle of this method for a hacker is that he will call the secretaryof the company and pretends to be a new employee who has difficulty gaining access to the system. Secretary (or other authorized user) may be inclined to this challenge and proud to be able to provide assistance to the new person at work [6].

Reverse social engineering

Very similar to SE, but differs in certain points. In RSE is necessary to have previous approach, such as business cards on which is number of social engineering as a service technician. RSE from SI differs in that if social engineer calls the user, the user is dependent on him and feels him to be grateful when SE is in the opposite [6].

Hunting based on trust and emotions

It is similar to RSE with the fact that if there is a user problem, they turn to the service. The attacker will help him and the user is thankful that he helped solve the problem, even if there is none. Employees should be very careful who they say important information [1].

Confidential tricks, cheats and personification

Another effective technique of social engineering involves employee fraud. Tricks may include arrangements header. This represents an apparent insertion of false statements in the mail system within an organization or Spoofing email address. In fact, the preferred method of contact is via e-mail [3].

Dumpster diving

Dumpster diving, meaning "browse garbage" is a common and often too easy way of getting information. Documents, which are common know - lists, organizational charts, basic directories, documents for official use only, political and technical manuals and personal statements. CDs, DVDs and hard drives are also appealing to attackers [3].

Computer infiltration

Computer infiltration is causing disruption of information systems in computers. Problems are more serious if the computers are networked [8].

Pop-up windows

Represent windows that open spontaneously on websites in which they are inserted. Sometimes they are too aggressive, that when you try to close them they will open more [8].

„419“aka Nigerian scam

Frauds of this kind are becoming more common. Business entity is approached by an electronic letter from countries in Africa or Asia with getting rich quick [8].

Spams

Spam is most often considered junk e-mail or junk newsgroup postings. For real spam is considered ad offering a product sent by e-mail or newsgroup. Unwanted e-mail from the company or website - is graymail. In Slovakia, we can meet with him at websites that provide discounts [8].

Phishing

This is a process that is used to when a hacker tries to obtain sensitive information. The term is taken from the word - fishing due to the similar method throwing bait and waiting for something that takes [5].

Baiting

Like the name suggests, the social engineer uses bait to entice its target to complete the action, such as clicking on a web link or insert the flash drive into your computer to trigger a Trojan horse. Baiting often relies on the curiosity or greed of the victim, as enticement to commit an act [5].

All computer systems must rely on human subjects, which are vulnerable characteristics. Regardless of such electronic devices safe from invasion, the lessons learned from the authorized user can do computer networks useless if used in an unauthorized manner. It is clear that knowledge of social engineering methods for employees, airline companies but also for all the people is very important. Important because of protect against him.

3. OPTIONS TO PROTECT AGAINST SOCIAL ENGINEERING

Preventing social engineering is a human issue rather than technical. According to Kevin Mitnick, the world famous controversial computer hacker who used social engineering in in about 50 percent of their offenses claimed that almost all social engineering attacks might not happen if employees would proceed in two steps:

- Check the identity of the person requesting - is it person who claims to be?
- Checking whether a person is entitled to receive information - is empowered to access the information?

Protection level employees

Airline employees, management and IT support teams must constantly take care of the safety and smooth operation of the company. It is necessary that employees regularly undergo educational training and be well informed about current risks and fraud. The intention here is to create a "human firewall" [2].

Security project

Is a comprehensive material, based on the current state of the information system and is used to manage information security and privacy in the airline and to prevent their theft, deterioration, or unauthorized use.

Safety directive and security project to the extent possible eliminate security risks that may arise collection, storage, and continuing to provide personal data of the persons concerned [13].

The social engineer may request information of different nature, with mentioned methods. This could include password, phone numbers, personal information, computer information practices and more. Before answering any of the questions on the social engineer the victim would be suspicious and think through whether a person is entitled to receive a response. If the victim does not know whether to answer and include current employees should refer to social engineer senior people who can either provide the information or not (see Figure 1).

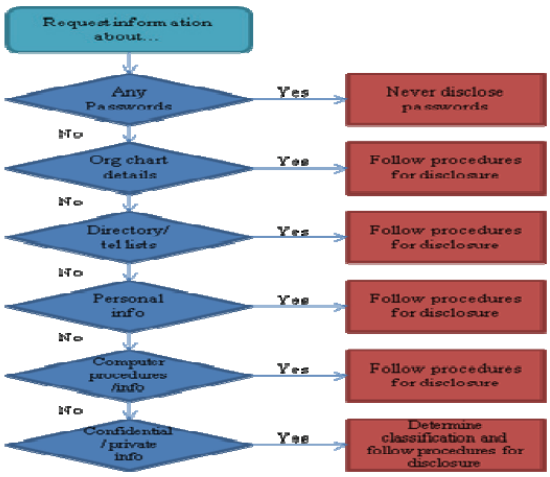

Figure 1 Flowchart requests for information.

Protection level management

Management should establish appropriate methods and procedures to prevent attacks social engineers. It should be established procedures for reporting incidents IT, so any known or suspected incidents should be reported immediately in order to minimize the threat. In addition, should lay down rules concerning the disclosure of information to third parties. Efforts should be focused on training and awareness rising on the release of information. This leads to the very fact that should be provided security training and awareness programs [2].

Protection level IT teams

Names and details of members of the IT team should never be published in a publicly accessible website. In addition, technicians must assign trouble tickets' (these are some reports from employees, which reported either defect or lack of information, which in turn solves IT support teams) in the relevant sections to avoid the lack of experience in a particular area. Another important area of interest is the account management. Careful record keeping is a must, because compromised account significantly increases the probability of fraud attacker to obtain information [2].

There are plenty of literatures on prevention of social engineering, but almost all preventive measures can be summarized in one word - verification. If all requests for information verified as to the identity and occupation, social engineering could become obsolete [2].

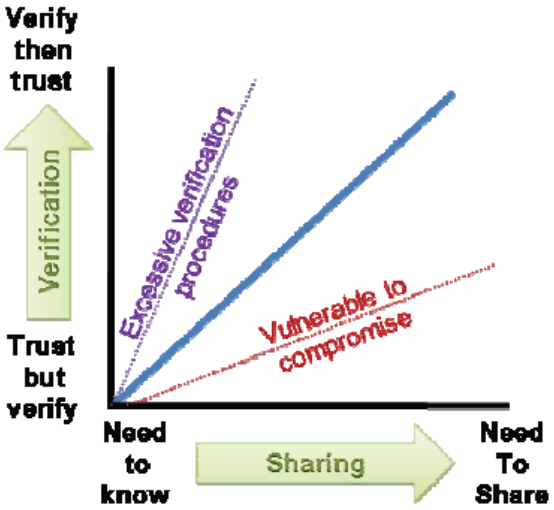

Figure 2 Relationship information sharing and verification.

Information sharing has a positive relationship with the verification. In other words, if this policy changes, increased information sharing. It is necessary increase verification procedures. Bold blue line (see Figure 2) represents an ideal relationship between sharing and verification. The more information we share, the more necessary verification procedures. In an environment where little information is shared, the phrase "trust but verify" may be sufficient, because information sharing is the exception rather than the norm. Purple line represents a situation where the verification procedures are too high for the amount of information that is shared, leading to ineffective policies and procedures. On the other hand, the more information is shared, it is necessary to increase verification. It is therefore necessary to

shift "verify, then trust" information security. The red line represents a situation where the information is shared more, but lacking commensurate verification procedures. Unfortunately, it is assumed that the current path is closer to the red line as the blue [5].

Protection against dumpster diving

Paper shredders are used to protect against Dumpster diving to prevent identity theft or to a maximum not facilitate the work of attackers taking advantage of social engineering. According to DIN 66399 know six data carriers (including eg. paper, CD, DVD, floppy, USB) and seven levels of security. Security level that produces a document shredder depends on cutting units [7].

Protection against Malware

If businesses and users will follow these procedures the safety of their property has increased:

- Starting current security software
- Getting the latest software updates
- Understanding the functioning of malware
- Enabling Firewall
- Restricting user rights [11].

Protection against trojans

Some practical tips to avoid becoming infected with trojans both for employees or the whole aviation companies:

- Do not download a files from people blind or from sites that you are not 100 percent sure.
- Even if the file comes from a friend, you still need to make sure that contains the file before opening it.
- One must be aware of hidden file extensions.
- Do not use in their programs to download or open files.
- Do not write commands blindly to infect others. Never go to a web address that brings strangers. Do not run the fancy programs or scripts.
- Do not let it calm down a false sense of security just because you are running an antivirus program.
- Finally do not download an executable program just to have looked out of curiosity [10].

Protection against Spam

We describe five best practices in the fight against e-mail spam:

- Keep more privacy to your email address - not including e-mail address in the text of the public internet chat rooms or anywhere on the website. If so only in graphical form.
- Select a more complex e-mail address
- Do not click on links spam e-mails
- Use a good e-mail filter - that will block spam [9].

Protection against Phishing and Baiting

With the combination of software to filter e-mails and employee awareness about security and best practices, phishing attempts can be detected and stopped. Employees should follow the following tips:

- Be suspicious of any e-mail that asks you to click on the link.
- Check the URL before clicking any link so that you pass your mouse over the link, and you examine the URL.
- Never open attachments unless it is verified.
- Delete any suspicious e-mail before opening it.
- Keep your computer software up to date.
- Make sure the computer's firewall is installed and running [12].

The prevention of social engineering achievements are aware policy and training. These instruments are closely related. We become more attentive before the attack surface of the social engineers develop policies against threats to communicate with each other and then we train people to know and to be able to protect to protect the library from social engineering [1].

Currently possible to define general recommendations for protection against social engineering:

- We should be suspicious of unsolicited communications relating to staff, technical information or other internal details.
- We should provide passwords or usernames by phone or e-mail no matter who you call.
- We should not provide information on persons anyone personally only to the person and only on presentation of a document or other suitable means of identification.
- If you're not sure whether the request is justified, let us turn to the relevant authorities.
- We should trust our instincts. If we have a bad feeling of the questions or communications, is probably never a good feeling.
- We should document and report suspicious communications.

5 DESIGN AND IMPLEMENTATION OF ELECTRONIC COURSE IN MOODLE

Based on the knowledge of social engineering, the methods and the proposed measures to protect against various social engineering methods and recommendations to the aviation business we have created a dedicated e-course, which should serve to raise awareness against social engineering threats. In order to be able to develop a course, we need to know the basic principles of the formation rate. Besides technical requirements which have to meet the electronic course, we were integrated and some additional requirements, such as: interactive, graphically simple and well-prepared environment, uncluttered and intuitive viewing electronic educational materials freely available in browsers with a suitably chosen resolution, simply executable applications [3].

5.1 The structure of the electronic course

Before we created an electronic course, we had to know for what purpose it is composed, for whom it is intended and how it will look its structure. Based on the information from the field of social engineering, we have proposed a model course structure (also with a description of the types of activities or resources used in Moodle):

Theme 1: Introduction
- The opening words of the course (website)

Theme 2: Social engineering (SE)
- Social engineering (lecture)
- SE based on people (lecture)
- SE-based technologies (lecture)
- Identity Theft and human psychology (lecture)

Theme 3: SE Methods and means of protection
- Direct application (lecture)
- Reverse social engineering (lecture)
- Fishing with based on trust and emotions (lecture)
- Confidential tricks, cheats and personification (lecture)
- Research (lecture)
- Dumpster diving (lecture)
- Computer infiltration (lecture)
- Phishing (lecture)
- Bait (Baiting) (lecture)
- Military scams (MILDEC) (lecture)

Theme 4: Possible protection against SI in the aerospace company
- Protection Model (lecture)
- Prevention in the aviation business (lecture)
- Employees of the airline
- Management of the airline
- Teams of IT support to the aviation company

Theme 5: Bibliography
- Bibliography (links to file / web page)

From the proposed structure we can be observed a large range of available lectures.

5.2 Implementation of electronic course

Moodle has several tools that allow input by the various types of training modules and materials. These tools are divided into:
- ***sources*** **-** such as, in the basic equipment, book title, page text, web page, link to a file or web page, link directory and IMS package.
- ***activities*** **-** such as, in the basic equipment, survey, database, forum, chat, written work, lectures, research, SCORM / AICC, vocabulary, test, and wikis assignment (file, on-line text and off-line activity).

Selecting appropriate resources and activities and the gradual fulfillment appropriate content, we gradually realized the entire structure of the electronic course. In individual subjects, we processed a total of 16 lectures, 43 links to files or web pages and one website. Within each lecture students are prepared for a few questions on the subject. On this basis, you may be able to test whether the subject mastered. Finally end of literature.

Created course on social engineering as can be seen in Figure 3 and can be found on Moodle Faculty of Aeronautics at the source: http://www.moodle.leteckafakulta.sk/course/view.php?id=242

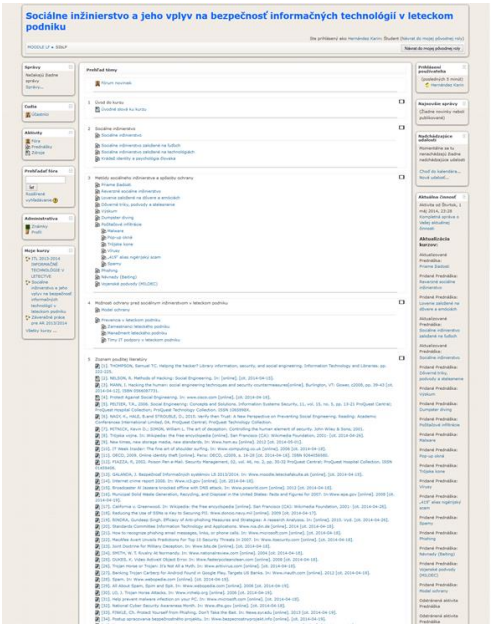

Figure 3 Implemented electronic course.

6 CONCLUSION

The primary objective of our previous solution was to analyze the methods of social engineering, to suggest possible protection against it and to create an electronic course in Moodle. We concluded that social engineering extends to all areas of human activity and, therefore, is to clarify this theme the best possible format for providing information for all students who use Moodle. For students but also the very businesses that will benefit. Students have the opportunity to acquire information from the problem and if they decide to work in organizations operating in aviation or another area, will have knowledge of the impact of social engineering on running your business, but also about the possibilities of how to avoid hazards. The organization can get the most out of it and avoid unpleasant situations and security threats.

BIBLIOGRAPHY

[1] THOMPSON, Samuel TC. Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries*. p. 222-225.

[2] OECD, 2009. *Online identity theft* [online]. Paris: OECD, c2009, s. 16-28 [cit. 2014-04-16]. ISBN 9264056580.

[3] NAGY, K., HALE, B. and STROUBLE, D., 2010. *Verify then Trust: A New Perspective on Preventing Social Engineering.* Reading: Academic Conferences International Limited, 04, ProQuest Central; ProQuest Technology Collection.

[4] ŠVEJDA, G., Z. PALKOVÁ, M. DRLÍK, T. BELÁKOVÁ a Z. HOTVÁTHOVÁ. *Vybrané kapitoly z tvorby e-learningových kurzov* [online]. Nitra: Univerzity Konštantína filozofa, Pedagogická fakulta, 2006 [cit. 2014-04-25]. ISBN 80-8050-989-1. Available on the internet: https://edu.ukf.sk/file.php/1/files/mo odle_tvorba_kurzov_UKF_Nitra.pd

[5] PELTIER, T.R., 2006. Social Engineering: Concepts and Solutions. *Information Systems Security*, 11, vol. 15, no. 5, pp. 13-21 ProQuest Central; ProQuest Hospital Collection; ProQuest Technology Collection. ISSN 1065898X.

[6] NELSON, R. Methods of Hacking: Social Engineering. In: [online]. [cit. 2014-04-15]. Available on the internet: https://www.hackerzvoice.net/ceh/CEHv6%20Module%2011%20Social%20Engineering/Social%20Engineering.htm

[7] New times, new storage media, new standards. In: *Www.hsm.eu* [online]. 2012 [cit. 2014-05-01]. Available on the internet: http://www.hsm.eu/us/products/shredding/document-shredders/new-din-standard/

[8] GALANDA, J. Bezpečnosť Informačných systémov LS 2013/2014. In: *Www.moodle.leteckafakulta.sk* [online]. [cit. 2014-04-15]. Available on the internet: http://www.moodle.leteckafakulta.sk/course/category.php?id=30

[9] All About Spam, Spim and Spit. In: *Www.webopedia.com* [online]. 2006 [cit. 2014-04-19]. Available on the internet: http://www.webopedia.com/DidYouKnow/Internet/spam_spit_spim.asp

[10] LO, J. Trojan Horse Attacks. In: *Www.irchelp.org* [online]. 2006 [cit. 2014-04-19]. Available on the internet: http://www.irchelp.org/irchelp/security/trojan.html

[11] Help prevent malware infection on your PC. In: *Www.microsoft.com* [online]. [cit. 2014-04-18]. Available on the internet: https://www.microsoft.com/security/portal/mmpc/shared/prevention.aspx

[12] FINKLE, Ch. Protect Yourself from Phishing. Don't Take the Bait. In: *News.syr.edu* [online]. 2013 [cit. 2014-04-19]. Available on the internet: http://news.syr.edu/protect-yourself-from-phishing-dont-take-the-bait-90416/

[13] Postup spracovania bezpečnostného projektu. In: *Www.bezpecnostnyprojekt.info* [online]. [cit. 2014-04-19]. Available on the internet: http://www.bezpecnostnyprojekt.info/bezpecnostnyprojekt_postup_spracovania.html

AUTHORS´ ADDRESSES

Hernández Karin, Ing., karinkocka@gmail.com
Galanda Jozef, Ing., PhD., jozef.galanda@tuke.sk

Department of Aerodynamics and Simulations
Faculty of Aeronautics
Technical University Košice
Rampová 7,
041 21 Košice