R&E-SOURCE http://journal.ph-noe.ac.at
Open Online Journal for Research and Education
Special Issue #4, December 2015, ISSN: 2313-1640

"COMPUTER SECURITY" and its importance in engineer education

Ildikó Pšenáková[*] *Veronika Stoffová*[†],

Abstract

The computer security is an important and actual problem in digital age. How can a regular user prevent cyber-attacks aimed at his/her computer or at other IT devices connected to the Internet? What should she/he look out for when browsing web pages not to become a victim of computer crime? The authors of this paper seek to answers these and many other similar questions. They propose to include topic of "Computer Security" not only into the curriculum of engineers such an object or as a thematic unit but also for future teachers of computer science.

"Computer-Sicherheit" und seine Bedeutung in Ingenieur Ausbildung

Zusammenfassung

Der Computer-Sicherheit ist ein wichtiges und tatsächliches Problem in digitaler Zeit. Wie kann ein normaler Benutzer zu verhindern Cyber-Angriffen auf seinem / ihrem Computer oder anderen IT-Geräten mit dem Internet verbunden ausgerichtet? Wie sollte sie / er Ausschau nach beim Surfen Internetseiten nicht ein Opfer von Computerkriminalität zu werden? Die Autoren dieser Arbeit versuchen Antworten auf diese und viele andere ähnliche Fragen finden. Sie schlagen vor Thema "Computersicherheit" nicht nur in den Lehrpläne von Ingenieuren sondern dieses Thema als eine thematische Einheit, auch in den Lehrplänen für Lehrer der Naturwissenschaften integrieren.

Keywords:
computer security
information security
e-learning
distance study

Schlüsselwörter:
Computer-Sicherheit
IT-Sicherheit
E-Learning
Fernstudium

1 Introduction

In the age of computer networks, such that any "personal computer" becomes "computer network" which is part of a vast web of interconnected computers, among which you can send, receive, exchange information without limitation. At present, unfortunately, we often encounter misuse of data or information resources

[*] Trnava University in Trnava, Faculty of Education, Department of Mathematics and Informatics, Priemyselná 4, 917 01 Trnava, Slovakia
E-mail: ildiko.psenakova@gmail.com

[†] Trnava University in Trnava, Faculty of Education, Department of Mathematics and Informatics, Priemyselná 4, 917 01 Trnava, Slovakia
E-mail: NikaStoffova@seznam.cz

stored on computers of different owners. "Thanks" possibilities of computer networks and malice of some users the public oft receives many non-public information of organizations and individuals.

The computer network is constantly at risk of infecting the computer various types of computer viruses, worms, spyware, and the like. Prevent or at least limit such ills (ailments) in the global computer network can only be a prudent computing. When the "literate" user falls victim to such attacks, will not allow their further spread and protect your computer from attack. In order to cope with user protect computer from external attacks, are necessary specific knowledge in computer security. Education in the field of protection against social threats and possible identity theft on computer networks for common – non-professionals practically non-exist (Pšenáková – Szabó, 2014).

2 Possible threats and attacks

Parallel with the evolution and development of information technology we have always emerged even people who tried to disrupt their activities, to break their safety. Intruders or attackers can be greatly simplified into two main groups. Some use their knowledge and experiences to harm persons or firms. Others are involved in industrial espionage and information obtained illegally trying to abuse.

The second group is those who believe, that all information should be free and freely available to all interested parties. They only simulate their attacks and use them for testing and improving the software system, even with the permission of the owner. Often they work as analysts and contribute to enhancing the security of computer systems.

There are also those attackers who can not easily move up and say whether they are good or bad. They work alone, quietly, without permission of the owner of the system. Their activity tries to point out holes or software errors in the programs. In addition to proving her/his skill, attackers have other reasons and motivations for this activity. For them, money is important, whether in the form of remuneration or ransom. Some attackers try to cause damage and avenge his former employer, he or leave a message just to prove that they are good in my resistance. The attacks are also used in competitive fight different companies.

The consequences of an attack can vary from simple harmless humorous notices to huge financial losses. For example, the banking system disruption or harm to humans manipulations hospital information system. If an individual becomes the victim of an attack may result in undesirable leakage of personal data and their subsequent misuse or alteration (Pšenáková – Genči, 2012).

2.1 Identity theft

One way, how to get to the foreign data is called ***Phishing*****.** Its principle is simple. The attacker sends the person e-mail, which is the impression that is sent from a trusted source such as a bank or an online store. The client asks to conduct checking of personal data, account numbers, access passwords or unlock accounts ***Internet-banking***. Mail and text look legit, and at first glance it is not always possible to tell that it is a scam.

Needless trust "**web site**" requiring personal information or fill multiple identifiers. The design of the false pages is similar to, for example, the official website of the bank. The user is asked to fill in some personal information: name, credit card number, PIN, credit cards and the like. Usually they are functional only a few fields that the client redirect to fake sites. If the client gives his data to such sites it is almost certain he will lose his bank savings.

Obtaining data stored in electronic devices is also possible by hardware theft. Theft of equipment suffered damage property, as well as mental as it fades important data and documents. Even stealing the identity of this method is a common and relatively simple. Users underestimated enough memory contents of electronic devices such as laptops, USB devices, CDs, DVDs, mobile phones and the like. For such devices, users store their personal information such as phone numbers, dates of birth, credit card codes, passwords, bank access, dates of meetings and other information that are the basis for the misuse of their identity. Another way is called **stealing identity**. Hacking, in which the attacker tries to compromise your system using redirects data or scan to a computer network and are uncorrected gain access to personal user data. **Keyloggers** are programs that record keystrokes on the keyboard and record as well as user names and passwords input.

2.2 Malware

"Malware" is the name for a group of malicious programs that are detrimental to most often by erasing data from computer storage devices. Malware is divided into four main groups:

1. ***A virus*** is a program that spreads itself in the computer's memory so that other programs and the infection causes various problems and damage, starting with the announcement of "funny" text on the screen and ending deleting all data in memory. To infect other computer virus needs a physical transmission medium, such as a USB, a DVD, and the like.

2. ***A worm*** is a program containing malicious code that attacks host computers, and can spread itself over a computer network.

3. ***A trojan*** attacking the Internet as worms, but attacks from within the network. On the outside it appears to be "harmless" document. Against compromise antivirus software protected so that they "enclose" the application program, and it is difficult to detect the source of infection. The system varies deleted malware can even open so. "Loopholes" and thus allow an attacker access to the infected computer without the recognized user name or password.

4. **Spyware** is a program that is built into useful applications and is used to obtain information such as a list of email addresses which can then be used for marketing purposes. Among computer users – non - professionals, those terms are often replaced by a single concept viruses. The reason is in our opinion that viruses have emerged as the first computer ills of this kind, and all the people causing problems of a similar nature included under this term. In principle, the name of the malicious program does not change the consequences of his action on the equipment, the point is to make users aware of it and started to defend against such attacks.

2.3 Denial of Service

Refusal or denial of service (DoS) attack is a technique for Internet services or the web site at which the overfilling requirements for that service or site that they then catch up, respectively fails to perform and consequently the service falls or at least is non-functional, respectively unavailable to other users.
The aim of such an attack can be:

- repeated reset the target computer;
- distributed communication between the server and the victim so that their communication was not possible at all, or to be very slow.

Distributed DoS attacks (DDoS) is characterized by targeted attacks trying to overwhelm reflection multiple computers. Often the attack is carried out without the knowledge of the owners of the attacking computer as to challenge the computers that have been infected beforehand. DoS and DDoS attacks are usually designed so that their aim is a time attack on one particular service, but there are also enabling distributed attacks at one time for more services.

2.4 Social engineering

Social engineering is a type of attack using people manipulation in order to obtain confidential information or performing a particular action on your computer. There are several methods by which social engineers attacked the computer of user. "Attack" can take place in direct person contact or by means of communication tool (phone, mail …). In this case is abusing the credulity of people. Attacker impersonates as a representative of the well known (existing) company or institution. The attack can be carried out through regulatory environment, for example by leaving storage media in an accessible place. The techniques used by social engineers as:

Baiting - technique is based on people's curiosity. The attacker left a portable storage medium with dangerous content on the site by the victim often passes.

Pretexting - fake fictional scenario, with the hope of obtaining information. In scenario it is also used some true information to persuade the victim.

Hoaxy - alarm messages, the messages are disseminated through the Internet, which ask to forward the massage.

Diversion theft - is a technique used by professional thieves. They are mostly directed against the courier and transport company.

Eavesdropping - interception of conversations and subsequent misuse of the obtained information.

Shoulder surfing - a technique that requires observation of the victim. It is oriented to observation of passwords, PIN numbers and other authentication important data.

Dumpster driving - Forward searches the garbage from which it may obtain information. Important unnecessary documents are therefore better to shred or destroy completely.

Belongs here already mentioned **phishing,** which mostly use the phone or e-mail. The attacker will perform as a representative of the well-known firms, banks and no confirmation about account information. **Defence against all forms of social engineering is almost impossible.**

3 Ways of defence – countermeasures

In this part of article, we present some basic advice and procedures to prevent such attacks and complicate the "work" the striker. Computers must be protected against unauthorized manipulation. We need to guard against creating illegal copies of computer memory contents, important data from theft or destruction. It is necessary to protect a computer against attacks and malicious software. Maintain the hardware and software it is possible to secure compliance with the three fundamental principles of defence:

Prevention

Prevention is the basic and most important step, which should ensure not only the physical but also the "mental" security of computer system.

- Room where is a computer system installed should be lockable (anti-theft) as a precaution against theft. In the case of notebook, it is necessary to guard it carefully, not only because of the financial loss, but also because of the possibility of misuse of the information stored on it (data theft).
- Permanent data backup can assist in system recovery after data loss.
- Using secure passwords (authentication and authorization) can greatly torment striker.
- Does not provide key information to unknown persons, mails with suspicious content directly delete (social engineering).
- Do not use a public computer to use Internet banking, because it threatens to decode the passwords, etc.

The best method to avoid data loss is a combination of software and hardware methods to protect.

Detection

Knowing the problem can be solved. To detect harmful malware there are special antivirus programs that are good for regular use. But it is necessary their permanent updates.

Remedy - Recovery and repair

Remedy and repair the damaged software is very important for safety work on computer, for use Internet services and for get relevant information for every day activities of user. Delete malicious software is ensure better safety. Also is important to learn from mistakes and to be more carefully (Pšenáková at al., 2012).

3.1 The malware defence

To protect against malware we can use suitable software. In order to achieve the required force, it is better to have specific program for each type of malware.

Antivirus software - monitors all the most important input and output points of system, which is the points through which viruses could penetrate the system. Its activity is going on in the background, -. a typical user can not notice his work.

Antispyware - used to detect and remove spyware.

Firewall - provides information transfer between a local computer network and the Internet. Firewall transmits data in both directions according to predetermined rules. Prevent unauthorized penetration into the local network and also not send data from it without the knowledge and consent of the authorized user. Firewall is a

kind of "computer customs" between local network and the Internet. Currently, the firewalls use is a very effective and important element in the protection of networked computers (Pšenáková, 2012).

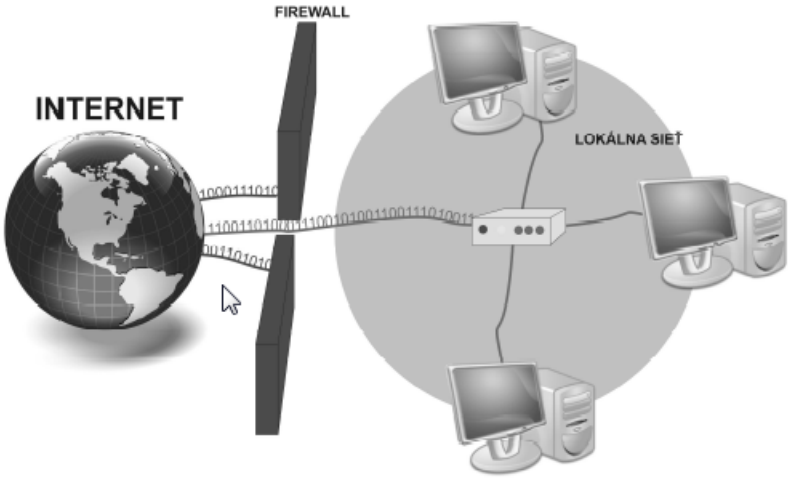

Fig. 1: Schematic representation of firewall principle

3.2 Defence against social engineering

In companies they are currently already commonplace identification cards, so should not get into the building undesirable persons. Base defence every company, every workplace at risk of such attacks, should be a security service at the entrance. Every employee of the company should control some basic rules of how to defend against social engineering. The best way of defence is vigilance in personal and electronic communications.

- Not to disclose confidential information to a person whose identity is not be verified.
- If in our office are also others, it is useful when entering credentials or PIN codes to use a keyboard cover.
- Never provide login information such as login names, passwords or other identification methods in the company, in the workplace, but even from their own private sphere.
- If the attack is held via email or phone asking for information confidentiality (passwords, request for sending documents ...) and by the seemingly credible and legitimate source, it is necessary to verify the credibility of a source other communication channels (call the number of known trustworthy person ...)
- Sensitive information that is no longer required but could still damage the company or person, you need to destroy.
- Portable media that if by chance found, it is better not to use or before applying scrupulously and rigorously to check their contents.

4 The necessity of computer security courses

In the before part of article, we only indicated most possible threats, attacks and ways to protect against them. In practice, there are many other and permanently creates new. The attackers are still coming up with new ideas and creating new more effective means than devalue work computer user such harm them and making life difficult

It is obvious that information security covers virtually all aspects of information technology - from hardware and software through systems architecture to organizational aspects related to the mode of operation of systems and user behavior. Solve most issues and problems in the field of information technology security it should be left to the experts (Genči at al. 2013).

In preparing engineers computing inclusion of a subject on cyber security in the study program it is guaranteed. In the case of an ordinary computer user it is not easy to obtain the necessary knowledge and experience in the field.

It is obvious that some knowledge of computer security is necessary, even essential for non-professional users of computer technology and information and communication technologies. It is therefore necessary to develop a course of computer security, for this category of users. The course should include not only current theoretical knowledge, but it should be containing also a practical training. Practical training should be geared to handle every dangerous situation and obtain certain information literacy for participant. He should learn and master the psychological and resist any attractive offer, visions of fabulous wealth, unimaginable winnings, inheritance and the like. The user of the computer to behave in every situation calmly, wisely and not rashly on order to his actions and spontaneous reactions not produce uncomfortable, irreparable, fatal consequences.

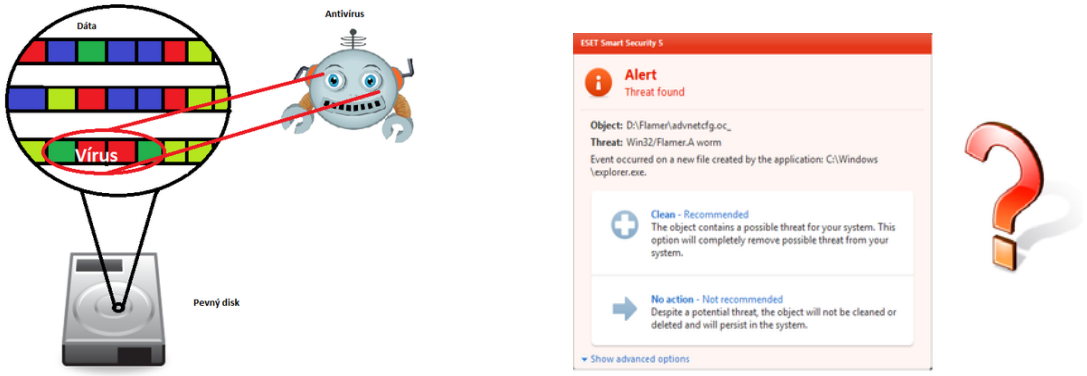

Fig. 1: Illustrative examples of pages of electronic course in computer security

5 Conclusion

The aim of the article was to highlight the importance of computer security and initiate the creation of electronic courses computer security for non-professionals. The course should be implemented in e-learning, and should provide for participants to basic information on potential threats to information systems and means of obtaining protection against them. At the same time, the participants had the opportunity to verify the knowledge gained by short tests.
Such courses should include (or should allow to pass) also situational training to master the many tricky and complicated situation during the attack. Virtual attacks should be carried out using simulation models to which the trainee should respond. User response should be evaluated and analyzed. They should explain not only the consequences in case of incorrect reactions such but should be shown the justified and correct procedures as possible solutions to simulated situations.

This study was supported by KEGA-grant: 010UJS-4/2014 Modelling and simulation in education.

References

[1] *Bezpečnosť na Internete*. [online]. 2012 [cit.2012-03-20].: http://melisko.webnode.sk/news/bezpecnost-na-internete/

[2] Genči J. et al. (2013).: Some Results of the Pilot Course of Computer Security for Non-professionals, ICETA 2013: IEEE 11th International Conference on Emerging eLearning Technologies and Applications, Slovakia. Technical University of Košice, ISBN 978-1-4799-2161-4, 365-368

[3] http://www.csirt.gov.sk/informacna-bezpecnost/navody-aodporucania/socialne-inzinierstvo-812.html

[4] http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

[5] Pšenáková, I., Genči, J. (2012) Kurz počítačovej bezpečnosti pre neprofesionálov. In: UNINFOS: Zborník prednášok z medzinárodnej vedeckejkonferencie, Trenčín: TnUAD, 2012. ISBN 978-80-8075-538-6, s. 90-96**7**

[6] Pšenáková, I. (2012). Bezpečne na internete . In: *Media4u Magazine*: čtrvtletní časopis pro podporu vzdělávání. ISSN 1214-9187, Roč. 9, č. X2 s. 33-38.

[7] Pšenáková, I., et al. (2012). Course Content of Computer Security, in ICETA 2012: IEEE 10th International Conference on Emerging eLearning Technologies and Applications, Slovakia. Košice: Technical University, 2012. 317-320 s. ISBN 978-146735122-5.

[8] Pšenáková, I., Szabó, T. (2014). Niektoré aspekty potreby kurzu počítačovej bezpečnosti pre neprofesionálov. In Science for education – education for science. Nitra Univerzita Konštantína Filozofa, Fakulta stredoeuropských štúdií.