Trakia Journal of Sciences, Vol. 15, Suppl. 1, pp 402-405, 2017
Copyright © 2017 Trakia University
Available online at:
http://www.uni-sz.bg

ISSN 1313-7069 (print)
ISSN 1313-3551 (online) doi:10.15547/tjs.2017.s.01.067

SECURITY IN TODAY'S VIRTUAL WORLD

P. Georgiev*

Department of Management and Quantitative Methods in Economics, University of Plovdiv “
Paisii Hilendarski, Plovdiv, Bulgaria

ABSTRACT
In the article, the author presents the hazards surrounding our most valuable resource, namely information. The world we have known has long been transformed imperceptibly and immersed in virtual existence surrounded by the technologies and techniques that govern us, our documents, our data and our everyday life. Information as a resource is more and more accessible even though it has a personal, secret corporate character or a national security status. Considering the above, it is good to build methods and algorithms to prevent or to have prevention various attacks in the virtual world, but also to educate people about basic hygiene in dealing with risky information resources, technologies, software applications, and more.

Key words: Information security, information protection, corporate information systems protection, information resources protection, virtual spaces

INTRODUCTION

The lack of careful study of this matter at non-specialized institutions of higher learning leads to ordinary users of various information systems overlooking the importance of the security aspect.

The advantages of immersing information technologies in the lives of the members of our contemporary society are more than obvious and this involves a strong need to solve various information problems related to the information security. Guaranteeing a level of security in different information systems can come in different forms, but it is always aimed at the development of three basic features: completeness (the information on which important decisions are based needs to be reliable and correct, protected against possible intentional or unintentional contortion), accessibility (the information and the relevant automated services need to be accessible and ready to respond when needed), and confidentiality (confidential information needs to be accessible only for the person for whom it was intended)

Information as a resource is one of the most potent stimuli for economic development. Having and using certain information at a certain time to certain purposes is the root of success. Information is the factor which determines the subject with better chances of success, or in other words, gives them a lead over the others. Given the current situation, a company has fallen behind if it has failed to adopt self-sustaining information systems. Even small and medium-sized enterprises have seen a rise in the use of software for specific purposes. All those integrated systems generate a vast amount of information in the local networks of the enterprises, in their computer workstations, and on the Internet. It is those open access repositories that are the object of malicious acts. It is inevitable that at a certain point they would experience an unauthorized access, loss, change, or another information-based action, which would lead to a small, or in most of the cases, major loss for the organization, usually financial.

Many types of malicious software are known to exist. Many more viruses, algorithms aimed at contortion and deceit, and other methods used to cause harm are coming into existence. The battle we lead on different levels requires us to be in know of the latest developments, or to be “up to date”

In the following paragraphs the known types of viruses and malicious software, they origins, their spread, the harm caused by them, and the protection against them will be presented.

***Correspondence to**: *Penyo Georgiev, Department of Management and Quantitative Methods in Economics, University Of Plovdiv Paisii Hilendarski, Bulgaria, **24** Tzar Asen, 4000 Plovdiv, +35932261341, penyo@uni-plovdiv.bg*

1. Threats and Dangers

The revolution in technology and communication has radically changed the world we live in. Information technology has profoundly altered our interpersonal relationships. The Internet connects communities from different parts of the world. Social media allows every individual to instantly share information with another individual wherever they might be in the world. And the World Wide Web provides us with a digital depository in which we can keep personal or professional information for free or by paying an insignificant amount of money [1].

The virtual-space vision that users tend to have often doesn't even come close to the multifarious reality of the virtual world. Their vision is illusionary because they believe that it is a mirror image of the real world. The threats are invisible, unexpected, and instant, and danger may lurk in any seemingly completely harmless file. This author is of the opinion that it is only prudent to number some of the well-known dangers and to offer proven reaction and prevention methods.

Globalization offers an unprecedented access to tools such as the Internet, satellite communications, transactions completed via electronic means, free movement of people across national borders, exchange of official documents, etc. Unfortunately, such opportunities turn into basic instruments used by criminal groups and terrorist organizations for the achievement of their own ends. The development of the current global processes makes the establishment of a connection between geographically distant locations possible. It also facilitates coordination, communication, and the reaching of information-based objectives [2].

1.1. Information Security

Information security [6][8] can be defined as a single body consisting of various aspects, which can relate to the information resources in a physical way – directly and purposefully, or unintentionally, as well as in the form of virtual interferences. Some of the most common and well-known threats are:

1) The physical security of the computer systems – theft or unauthorized physical access; natural disasters; technological failures caused by damage or external circumstances.
2) Internal threats coming from one's own personnel – unintentional technical mistakes; other types of mistakes and social engineering; malicious employees.
3) Malicious acts of third parties – hackers and crackers; unauthorized access via means of passwords.
4) Phishing
5) Malicious software (viruses) – resident viruses; boot; direct-effect viruses; stealth; macro viruses; logic viruses; time-bombs; MBR (Master Boot Record); BIOS viruses; pseudo-router viruses; information pollutants; polymorphic viruses; bio-computer viruses; binary viruses; RAM viruses; companion viruses; killer viruses; fat scramblers; Java viruses; E-mail viruses; WAP viruses; worms; host worms; Net worm; Trojan Horse; droppers; bombs; INI programs; BAT infections; backdoor; spyware; adware; keystroke logging/screen logging; rogue; root kit.
6) Identity theft
7) Passwords are not secure enough
8) Passwords are inconvenient

1.2. Security or Hygiene When "Surfing'' the Virtual World

The security of information [3] requires it to be protected from its creation to its destruction. It is advisory that security is established on all levels, starting with the most basic hardware level or network security[7] level, up to securing data itself. Information can be basically classified as Public Information or Official Information, but it can also be Confidential Information. We can easily see the necessity for an introduction of standards for the management of information resources protection systems from the previously discussed points. Such active standards can be purchased from the Bulgarian Institute for Standardization (BDS) [9]. All of the adopted systems and rules are expected to adhere to the laws and legal acts of the Republic of Bulgaria.

1.2.1. Legal Acts

1) Classified Information Protection Act, 45/2002
2) Personal Data Protection Act, 1/2002.
3) Ordinance on the mandatory general conditions for security of the automated information systems / networks in which the classified information is created, processed, stored and transferred, a decree of the Council of Ministers № 99/10.05.2003, 46/2003.
4) Regulation on the Cryptographic Security of the Classified Information, 102/21.11.2003
5) Rules for the Application of the Classified Information Protection Act, a decree of the

Council of Ministers № 276/02.12.2002, 115/10.12.2002.

6) Doctrine on Communication and Information Systems of the Bulgarian Army, 2001, adopted by the Defense Council, Protocol № 4/04.03.1999.
7) Concept of Information Strategy of the Ministry of Defense, adopted by the Defense Council, Protocol № 6/20.04.1999
8) Concept of information activity of the Ministry of Interior, State Gazette, 38/30.04.2001.

1.2.2. BDS Standards

1) BSS ISO/IEC 27000:2016 – Information Technologies. Security Methods. Information Security Management Systems. General Overview and Dictionary – price: 81.60 lv. *(*BSS *ISO/IEC 27000:2016 replace and revoke* BSS *ISO/IEC 27000:2014 on 2016-03-17)*
2) BSS ISO/IEC 27001:2013/Cor. 1:2016 – Information Technologies. Security Methods. Information Security Management Systems. Requirements. Technical Correction 1 – Price: 0.00 lv.
3) BSS ISO/IEC 27001:2013/Cor. 2:2016 – Information Technologies. Security Methods. Information Security Management Systems. Requirements. Technical Correction 2 – Price: 0.00 lv.
4) BSS ISO/IEC 27001:2014 – Information Technologies. Security Methods. Information Security Management Systems. Requirements – Price: 59.60 lv. *(*BSS *ISO/IEC 27001:2014 replace and revoke* BSS *ISO/IEC 27001:2006 on 2014-05-19)*
5) BSS ISO/IEC 27003:2011 – Information Technologies. Security Methods. Instructions for the Adoption of Information Security Management Systems – Price: 140.00 lv.

Other standards for Information Security Management Systems can be found on the official site of the Bulgarian Institute for Standardization, but their status has been revoked.

1.3. Rules of Hygiene We Need to Follow

It is understandable that a universal solution, which can protect and completely secure certain information, is difficult to find and does not exist up to this point. There is no such method or software application which can provide ultimate security and it is unthinkable to try to find one, keeping in mind the diverse and vast nature of the virtual world. There are different kinds of secured virtual environments, but this is due to their access points being controlled. An example of this type of environment is the Virtual Education Space VES [4][10].

The author finds it prudent for the different management levels of the organizations to adopt either the standards mentioned above, or practices and procedures in accordance to their own activities. Special attention is paid to the organization of the company's information systems and their protection[5], as well as to the training of employees which should be a more widely-adopted practice in the institutions of higher learning.

1.3.1. Measures for the Implementation of Information Security

1) Administrational measures (organizational, procedural);
2) Logical (technical) measures;
3) Physical measures
4) Management measures
5) Access control – authentication – flexible authentication; smart cards; phone authentication; biometric authentication, etc.

1.3.2. Security Procedures

1) Physical security
2) Personal security
3) Document security
4) Marking and report of classified information in automated information systems (AIS) and in networks
5) Registration, marking, report and destruction of material storage mediums used to store classified information
6) Communication and cryptographic security, protection against parasitical electromagnetic radiation.
7) Basic computer security requirements
8) Security modes
9) Security during the exploitation and development of certified AIS or networks
10) Security of AIS or networks in which information classified as "top secret" is generated, processed, stored or transferred.
11) Possible replacement of the computer security measures

1.3.3. Security in Computer Systems and Networks with Internet Access

1) Reliability of the information
2) Virus check
3) Technologies which allow for automatic up-dates
4) User's spoof
5) User's anonymity
6) Java
7) Change of web pages

1.3.4. Technical protection measures

1) Cryptography
2) Shielding
3) Using terminals
4) Using an uninterruptible power supply

1.3.5. Recommendations for the users

1) Enable Data Execution Prevention (DEP)
2) Don’t disable User Account Control (UAC) in Windows
3) Consider switching to a standard/limited user account
4) Do not disable the inbuilt Windows Firewall
5) Keep your software updated
6) Disable the auto play function in Windows
7) Do not frequent suspicious websites and P2P networks and do not download cracking tools.
8) Use additional protection software
9) Beware different video files or online videos which require a specific codec in order to be played
10) Beware spam messages in messaging applications or sites which you use (particularly Skype)
11) Use Facebook less often or not at all.
12) Download programs from reliable sources only
13) Keep the system partition updated
14) Secure your passwords
15) Set file encoding
16) Enable the IP Security protocol
17) Demand Secure Socket Layers (SSL) in web transactions
18) Demand a secure electronic mail
19) Use antivirus software
20) Don’t use public Wi-Fi networks if you haven’t installed a virtual private network (VPN)

CONCLUSION

Hand-in-hand with real threats in the real world increasingly often come threats originating in our computers, mobile devices, and the World Wide Web and they are no less dangerous that the material ones. The prevention against such threats should be systematic and consistent with clearly-defined rules and objectives. The establishment of a single, cohesive strategy of reaction and prevention against virtual threats is essential. This is especially true for big corporations and increasingly true for small and medium-sized enterprises. It also holds true for the ordinary user and their personal data. The basic information threats are well-known: malicious software, disloyal employees, human error, technical malfunction, external attacks, etc. The author finds it necessary to have a set strategy and tactical plans for the protection of information in small and medium-sized enterprises and for the protection of personal data. Thus, he intends to further his studies in the matter.

REFERENCES

1. I. Savov: The Collision of national security and Privacy in the Age of Information Technologies, CEPOL - European Police Science and Research Bulletin, issue 15, 2016
2. I. Savov: An overview of methods of collecting information in the field of national security, poceedings , National Military University „Vasil Levski”, 2016
3. Ts. Semerdjiev: Security and Protection of Information, "Classic and Style", Sofia, 2007, ISBN: 978-954-327-034-7
4. S. Stoyanov, A Formal Model of Virtual Education Space, international conference from delc to velspace plovdiv, 26–28 march 2014, 285-297 pp., ISBN: 0-9545660-2-5
5. D. Arnaudov, A. Krumova: Security and Protection of Information Systems, VFU "Chernorizets Hrabar", Varna, 2007.
6. Ts. Semerdjiev: Information Security, Softtreid, Sofia, 2004.
7. S. Stanev and S. Zhelezov, Computer and network security. Shumen University "Episkop K. Preslavski", Shumen, 2005, ISBN 954-577-306-5, 132 pp.
8. http://www.tuj.asenevtsi.com/Sec2009/Sec01.htm
9. http://www.bds-bg.org
10. V. Ivanova, A. Toskova, A. Stoyanova-Doycheva, S. Stoyanov, M. Veselinova, Lifelong learning in Virtual edication space with intelligent assistants, 8th Balkan Conference in Informatics 2017 (BCI2017), Skopije, Macedonia (to print).