COMPUTER NETWORK SECURITY AND ITS FUTURE

Radoje Cvejic[1], Velimir Dedic[2], Milena Kukric[3], Dragana Bankovic Djukic[4]

[1]Faculty of Strategic and Operational Management, Belgrade, Serbia
[2]Faculty of Strategic and Operational Management, Belgrade, Serbia
[3]Faculty of Business Studies and Law, Belgrade, Serbia
[4]Faculty of Business Studies and Law, Belgrade, Serbia

Abstract: *Since computer network of an organization connects to other networks via the Internet, network security is one of the most important factors which must be taken into consideration because an attack on any organization network can be undertaken both from inside and from outside the organization. That is the reason that computer network security is very important to prevent and protect the organization from attacks. The purpose of this research is to predict the future of computer network security for theperiod of next 5 years (2015-2020) with the use of Delphi technique, a widely used and accepted method for achieving convergence of opinion regarding real-world knowledge from experts in this field. The research result can be used to improveand develop computer network security including staff, hardware, softwareand privacy system.*

Keywords: *Network, Security, Trend, Delphi technique*

1. CURRENT SITUATION OF OUR COMPUTER NETWORK SECURITY

1.1. The idea of a computer network security

The computer network security of which we are talking about is actually network security, significant data in the system of network and the structural components of the network. Achieving security of computer network actually means protecting user data and computer systems from attacks and data theft out of computer network. People who work on protection of computer networks are engineers of technical and material safety analysis of computer system. They protect the system of the network from problems related to computer security that could affect computer's security of individual users, such as theft, crash or interfere with the operation of the system and so on.

1.2. Current situation regarding to the development of computer network security

Today, computers are popularized and represent necessary part of life of every man. People use the technology of communication through computer networks to communicate with their friends, in order to complete certain tasks in order to learn something new, or simply to have fun. The development of computer technology is changing the way people live and improves their quality of life. Yet, the security of the computer system still worries people. For China and the rest of the world it represents a serious problem. There are many experts in security of computer systems that implement serious research of security of computer system. They conduct special research for maintenance, destruction and repair of the security system of computer networks. Based on these studies, experts have built PPDRR model of computer network security.

Designing the security of computer networks involves in itself a wide range of specialties. Any profession which implies knowledge of computers could participate in this. For example, the creation and development of computer software, control and maintenance of software, could benefit from the protection afforded by the security of computer networks. Protection of security of computer networks can provide protection for developed technology and prevent economic losses. Therefore, many experts in the field of security computer system work on the creation, protection and research in the field of computer security system of computer networks, hoping to find an effective way of ensuring the security of computer networks or a way that would help to investigate and discover the striker of system computer network. Through numerous studies, experts have proposed a new method of analysis of security networks - "tree invader." Experts integrate information on past attacks and expresses them using mathematical formulas. This type of method is called "the tree of the attackers." However, this method still has some flaws and there are disagreements related to integrating and explaining the "sheets". Therefore, certain researchers have suggested so called. "graph privilege", a method of analysis which should improve all the previous methods and analysis of security of computer networks. The development of technology has led to constant innovation in the field of analysis method of computer network security. Building a computer network security system was also constantly developing. However, there was no specific method of analysis and model that could solve all the problems related to the security of computer networks. But scientific research in this field continues. People are still working on a model of computer network security.

In the last few years, most of the organizations have built a computer network they use every day. This is called local network which provides access service to members of the organization. Significant application that in this network is used is the Internet that connects all users within organization who can work together on that way. Moreover, the schedule of work within a team, called the Working Group, plays a very important role; each team has its own information system and server that contains important information. Work on the level of working group has goal to bring together specific groups such as, for example, team for sales, accounting, manufacturing, finance, etc. Intranet, or internal network includes all these groups together as an organization's private network used for sharing and exchange of information, something we call the online process work. However, the scope of the network is not limited only to the organization. Almost all organizations connect their internal network to the Internet so they would be able to cooperate with other organizations which

represent a way of improving the impact speed and convenience of work. Many organizations have their own websites in order to promote their products and services. Orders and providing services after sales will receive and send directly over the network.

Currently, many computer users erroneously believe that wall protection (so-called "firewall") can 100% protect network system, but, in fact it is not sufficient. [1]. For example, the administrator puts or sets the "rules of the firewall" to block access to web servers by allowing connection on port 80. This can prevent a problem on the network when hackers try to attack the ports 139 or 445. But if a hacker tries to attack a web application using port 80, and there is so-called vulnerability, he can attack the web server and wall protection or "firewall" would not receive any warning that is displayed to users. Therefore, SOU (Intrusion Detection System) is proposed as a kind of alarm. It will display a warning when it detects an attempt of attack on computer network. Other SOU called SOSU (system for intrusion detection and prevention attacks) or OSU (detection and prevention attacks) is a device used for the simultaneous detection of multiple attacks on computer networks by monitoring and analyzing network traffic. This study uses the Delphi technique [2-7], the scientific method for collecting information from the group of experts, which many people are trying to study and analyze the collected knowledge so they could predict the future in different areas, especially in science. Science and technology are constantly changing. Research by using the Delphi technique is considered to be the future science (Futurism), by putting emphasis on detailed research in order to gain a better knowledge and understanding of the future. In addition, it can alert the user to unpredictable things that can happen in the future.

The purpose of the research is to predict the expected future and to seek ways to prevent, control and improve so that we could be able to respond to future needs appropriately. In this paper, the Delphi technique was used to predict future trends in the areas of security network of the organization over the next 5 years (2015-2020). This research uses the questionnaire in order to investigate the opinions of experts in the field of computer network security organization.

2. RESEARCH METHODOLOGY

Steps in the methodology of the survey are shown in Picture 1. Delphi technique was used to explore the security of computer network of the organization over the next 5 years. We started by examining and gathering information about the safety of computer network of organization and of the Delphi technique too. Next step is implemented in a manner which is described in following text.

2.1. Research procedure

This research focuses on future trends in the field of computer network security organization in the next 5 years (2015-2020) using the Delphi technique. Future trend involves collecting thoughts of experts in the field of computer network security organizations using statistical approaches. The research methodology uses the Delphi technique presenting a form of research, to explore future trends together with experts that can provide worthy and reliable information. Three sets of the questionnaire were carried out in the way described in part 2.2.

Qualifications of experts - these people has knowledge, they are known and have experience of at least five years in the area of security of computer networks. Each expert will respond individually to 3 sets of questionnaires. We selected 17 experts in field of computer network security organizations, as a sample and they are divided into two groups;

1. Eight experts from government agencies and state enterprises

2. Nine experts from private companies
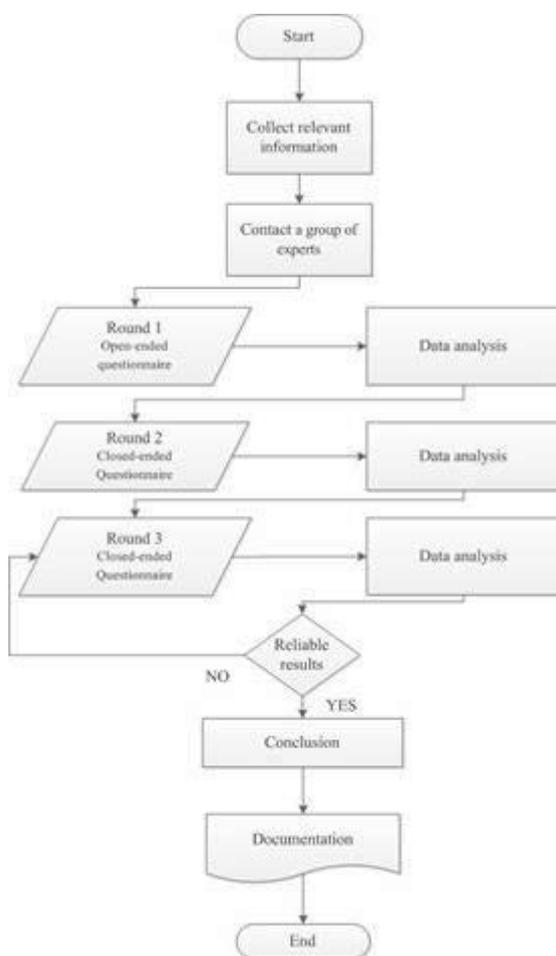
Picture. 1. Research procedure.

2.2. Questionnaires

In this section we develop a questionnaires that was used as a research tool and they are divided into the following three steps: In the first questionnaire which is open type, it has been opened the issue of security of computer network of the organization for a period

of 5 years (2015-2020). The questionnaire was divided into two parts, the first part of the question is about the problem of computer network security organizations in today's market, and in the second is the question of security of computer network of the organizations over the next 5 years (2015-2020). Next, we take the data from the first series of questionnaires by assessing direction of response of every individual expert on the questions from task so that we can evaluate whether their answers are moving in the same direction. If we have right answer, the question from the questionnaire would be included in the questionnaire of closed type. Then, the experts respond to individual sentences from the questionnaire with one of five possible answers or stands: 5: "strongly agree", 4: "I agree", 3: "I'm not sure," 2: "I do not agree" and 1 "in general I do not agree ", so that we could discover their views.

Then we calculate the middle value and ranges between quarters. After that, the third series of questionnaires will also be in the form of closed questionnaires in order to select those answers of experts that are designated with five points where the definition is the same as in the previous survey but middle values and medium ranges between quarters are added. The purpose of this is that groups of experts compare and validate their positions from the questionnaires given in the second series. Processing of these data give us a range between the quarters 0-1, indicating the accuracy of results which led to the final processing of data in order to obtain the final results.

SURVEY RESULTS

The research results can be summarized as follows:

3.1. Security of computer networks in the organization today

Today, every organization focuses on technology rather than on process or network security policy management within the organization. The result is that network security is not efficient. Most of organizations are careless when it comes to personnel responsible for the security of the computer network of the organization. Therefore, the employees in the organization do not comply with safety rules completely. Therefore, the security of computer networks in the organization is ineffective and inefficient. The security of computer networks can prevent at a certain level, but insufficient, the emergence of damage and that should be improved in the future and in many parts. The price of the equipment used for the safety of computer networks is too high. Therefore, it is difficult to reconcile the budget and resource estimation. Some managers will hesitate to install safety devices for computer networks, regardless of whether the security of computer networks is their focus or not. Each organization will often focus on pre operation and effect of the computer network in the organization than on its security. The real picture of computer network security depends on the ability of the staff responsible for the network in the organization. There is no dedicated staff working only on the security of computer network in an organization. Segregation of duties, understanding and making decisions of staff are really confusing. The result of all this is the fact that the security of computer networks in the organization today is ineffective.

3.2. Future of security of computer network in the organization over the next 5 years

Security of computer network in the organization should have a clear policy and sanctions. Moreover, all personnel in the organization should be strictly observed with that. The fact that there is widely accepted standard can be used to check and validating the security of computer networks. Persons who works on the security of computer networks in an organization should be experts knowing how to perform their duties and they should have the appropriate certificates of knowledge related to computer network security in the organization, which would be gained with exam of the appropriate test in front of an organization responsible for the global standard in the field of security. Devices that are used in computer network security in an organization should be of high quality having a high level of performance, and reasonable prices too. Besides that, they should be supporting the centralization of management so that they can be controlled and that they can be managed centrally, which includes an overview in real-time and efficient compatibility with other devices. They should also check that unusual movements in real time in terms of access or text on a variety systems or equipment, and to provide support for any security protocol related to the security of the computer network of the organization.

The software or program that is in a function of the security of computer networks in the organization and software which is used in the network should be able to check their operations and to be support of security of computer networks in an organization compatible with any other devices or software which serve the security of computer networks. They should be also supportive of the central management system and they should always increase efficiency on a high level being modern too. Besides, the price of hardware or equipment should be reasonable. Policy effectiveness of system in the organization should include a login (JP) and it should be at a high level, stable, fast and safe. Last but not least, is that at any moment it must comply with applicable laws of computers and being modern and not outdated.

4. CONCLUSION

In this study, we use the Delphi technique in order to predict the future of security of computer networks for the period of next 5 years (2015-2020). Questionnaires were three series including open and closed questionnaire, which was used to collect the opinions and stands of a group of experts. Results show the security of computer networks of today and for the next 5 years (2015-2020). In conclusion, the results showed the importance of staff, hardware, software and privacy, which is all significant to anyone who is concerned about network security. This will allow managing and control of important aspects for contentment of future needs and security problems related to the computer network of the organization.

5. REFERENCES

[1] C. C. Hsu and A. Brian. The Delphi Technique: Making Sense Of Consensus. Practical Assessment, Research &Evaluation Volume 12, Number 10, August 2007, ISSN 1531-7714. Retrieved March 25, 2011from http://pareonline.net/pdf/v12n10.pdf.

[2] Network security, Wikipedia, Retrieved March 25, 2011 from http://en.wikipedia.org/wiki/Network_security.

[3] S. Dixit and P. K. Jha. Network Security: It is a process, not product. SD Bansal College of Technology, India, 2009.

[4] C. Pangchan. Master in security. Info Press, Bangkok, 2008.

[5] T. Chomsri. Computer Network Security. Pro Vision, Bangkok 2010.

[6] CERT Coordination Center, Home Computer Security. SoftwareEngineering Institute Carnegie Mellon, November 22, 2002. Retrieved March 25, 2011 from http://www.cert.org/homeusers/HomeComputerSecurity/.

[7] C. Okoli and S. D. Pawlowski. The Delphi method as a research tool: an example design considerations and applications, Department of Information Systems and Decision Sciences, Louisiana State University, Baton Rouge, LA, USA, 2000.

[8] G. J. Skulmoski, F. T. Hartman and J. Krahn. The Delphi Method for Graduate Research. Journal of Information Technology Education, Volume 6, 2007.

[9] M. Tiantong. Delphi Technique. Faculty of Information Technology, King Mongkut's University of Technology North Bangkok, Retrieved March 25, 2011 from http://it.kmutnb.ac.th/monchai.

[10] Delphi Technique [Electronic version], Retrieved March 25, 2011 from http://202.143.130.99/files/Delphi3.pdf.

[11] H. A. Linstoneand M. Turoff. Delphi Method: Techniques and Applications [Electronic version], 2002, Retrieved March 25, 2011 from http://is.njit.edu/pubs/delphibook/delphibook.pdf.