ZRÍNYI MIKLÓS
NATIONAL UNIVERSITY
Doctoral Council

VALÉRIA PÓSERNÉ OLÁH

Information security aspects of information systems for public administration

PhD thesis booklet and
her official reviews

Budapest
2011.

ZRÍNYI MIKLÓS NATIONAL DEFENCE UNIVERSITY

VALÉRIA PÓSERNÉ OLÁH

Information security aspects of information systems for public administration

PhD thesis booklet and
her official reviews

Supervisor:

Prof. dr. Zsolt Haig, eng. colonel, PhD

Budapest
2011.

The scientific problem

Because of the information systems are commonly used in every aspects of human life, that is why in the era of public administration they take part in growing scale. Due to the personal computers and the lesser or bigger networks forming of them, the creation of the first viruses, the speeding up development of information technology the matter of information security became more complicated. Our NATO and EU memberships make great demands of newer information security in the used information systems of Hungary, amid the information systems of the public administration.

It is obvious, that the information security is effective, if it is ensured commonly for every element (servers, clients, operation systems, software, network, etc.) of the information system. However, the information systems of the public administration are far from the equal high level defense. There are areas where the usages of the modern defense methods are the same in quality, quantity and forms, but there are several information systems, where you cannot find the basic security settings. The significance of the shortcomings of the security of the information systems of the era of the public administration is quite big enough, because an incident can cause harmful effects for mass of people or for the whole society. For example, nobody would be happy if anybody would be able to acquire his / her birth certificate – due to the security problems of the system – which can be used to steal a whole identity and to take advantage in various ways.

By the very start of my research I could identify that the information systems of our public administration contain more and more vulnerabilities as other systems, and the attackers, their tools and methods develop in an immense pace.

The explorations, analysis of the threat on the information systems of the public administration, the inspection of the adaptability of modern defense methods need scientific research.

Objectives

I set the under mentioned aims in the course of my research:

1. Observing the information systems of the organizations of public administration, by modeling the system presenting and analyzing their functioning processes, the used

information security rules and the aspects of the staff operating them; exploring their lacks and defining the possible directions and results of their development.

2. Analyzing the possible attackers, the types of attacks against the information systems of public administration, and by this systematizing and grouping the threats.
3. From the viewpoint of information security analyzing, valuing and comparing the most used open source and close operation systems in the information systems of public administration and suggesting more possible application areas.
4. Based on the risk analyzing model observing the modern defense solutions used in information systems of public administration, their processing principles and suggesting adaptability enlarging the information security of information systems for public administration.

Applied research methods

I started my research **by gathering, systematizing, analyzing information based on wide scale literary research** of vulnerability of information system, later on I complement them whit the exploration of these vulnerabilities, and the **accomplishment of simulation based on modeling** and demonstrating of effective defense from the threats. I **followed with attention** the already done and ongoing dissertations based on the theme, the statements of scientific student essays, technological publications, scientific exhibitions and programs. I utilized the pieces of information and experience I gathered from the **interviews** of top managers of the social service sector. While I made this essay I lean on the national and EU laws, rules, standards and regulations of the information defense. I consulted, gathered experience, and **I used the experience from teaching** the subjects in creating, operation and auditing and reviewing safe information systems, for the creation of this document. I strived to reach and achieve my goals of this research by using methods such as **analyzing, synthesizing, inducting and deducting** several outcomes of researches and essays.

Structure of the thesis

I summarized my research for reaching the goals in an essay in the following structure:

1st chapter: I defined, specified the notions used in the essay, I observed the information systems of public administration and their working processes, I created the functional and

structured model of information systems of public administration and I defined the necessary aspects and tasks needed to form information security strategy strengthening information security of organizations in the civil service sector, I presented a possible option of strategy build-up and I explored the shortcomings of regulations of the information systems of public administration. I suggested solutions for eliminating the shortcomings.

2nd chapter: I analyzed and grouped the threats and attack methods against information security of information systems of public administration, I observed the attackers, targets, effects of attacks and by testing I analyzed and compared the most commonly used open source and closed operation systems utilized in information systems of public administration, then I drew the inference for their further adaptability.

3rd chapter: I observed the modern defense solutions usable in information systems, their working methods, than by the purposed, particular risk and effect analysis concentrated on the threats and defense lacks I suggested solutions for their adaptability to develop security of information systems for public administration.

At the end I summarized my conclusions, my main statements, I formulated the new scientific results reached by me and made suggestions for further usage.

Conclusions

After identifying and clarifying the basic expressions **I created the functional and structural model of information systems of the public administration.**

I presented the Electronic Government Backbone which is the basic infrastructure of e-governance and I analyze the Ügyfélkapu.

After observing the basic processes of the information systems I stated that the most critical points in the information systems of the public administration are the processes of putting in the data to and getting out the data from the systems. The proper regulating of these processes could enlarge the level of the information security significantly.

By studying the requirement system of the information security of the framework for e-governance I analyzed the basic conditions of setting up and maintaining the organizational information security and I formulate the goals and requirements of the information security strategy, I presented a possible build-up, the most important tasks to do according to the goals and the questions of the regular review of these tasks.

I examined the current and normative orders of government and the matters of their ancestors in the aspect of information security of the information systems for public administration and I stated that there are still some shortcomings, and the proper implementations on the lower level do not come or come partially into existence, and I see the reason of this mainly in the lack of suitable specialists and the lack of financing.

According to the previous issue I suggested working out a law of information security which is based on international standards and good case practices and regulates widely the information security of the organizations of the civil service sector, furthermore I suggested setting up an information security organization of experts doing inner auditions and consulting.

I examined the state of development of security consciousness of humane side which takes part in creating, regulating, processing and utilizing the information systems of public administration and I stated that problems of approach impede the creation and maintenance of proper information security, that is why I suggested introducing methods aiming to change it.

After clarifying the main steps of attacks against information systems I analyzed, systemized and grouped the threats, the scale of attackers, the targets and the methods and effects of attacks of the security of information systems of public administration. I observed and analyzed the opportunity of outer attacks in the aspect of exploiting the vulnerability of the network, operation system and installed applications, as well as I observed the diverse opportunities of inner threats and the accomplishable forms of attacks of combination of the previous two mentioned issues.

After that I wanted to reply an actual question, which refers to the expedience of the usage of open-source or closed operation systems on the computers of information systems of public administration. That is why I tested, observed and compared several services of operation systems of servers mainly used in information systems of public administration in the aspect of secure usage and I stated that the utilization of open-source operation systems may cause cost-cutting in purchasing software, its skills are not worse than the security services of closed operation systems. However the expertise is missing for the secure operation and it would be a problem to retool the self-developed, Microsoft based applications of the civil service sector and with this a big amount of vulnerability could come into the system, also thence these are more likely targets of attacks.

I stated that there are no essential digressions in the used methods, instruments and motivation of attackers considering the attacks of information systems of public administration or company. I see basic differences in one hand in the effects of differences

between the stored-processed information, on the other hand in the negative effects caused on the governance by the threats of availability, and finally in the negative effect of operability of public administration by the threats of cyber warfare.

I observed and valued the modern information security solutions, with statistical data I stated that these are not or partially used in the information systems of public administration.

I made a purposed, particular risk and effect analysis concentrated on the threats and defense lacks revealed in the previous parts of the essay, with its outcomes I suggested implementing, enforcing the upcoming security solutions in the security systems of every organizations of the civil service sector:

- Implementing central controlled, integrated end-point protected solutions and creating central controlled software refreshing architecture for reducing on a bearable level the threats caused by malfunctioned or manipulated applicator vulnerabilities, vulnerabilities created by system programs or by the vulnerabilities getting into system from remote computer;
- Creating screened subnet firewall architecture processing with application level firewall for lowering the risk of unauthorized admission into the network;
- Utilizing admission detecting and preventing tools to detect and parry unauthorized admission tryouts and attacks on the inner network;
- Implementing integrated central applicator and access management systems for lowering risks by unauthorized data access;
- Implementing encryption and automated saving system for reducing on a bearable level the risks caused by loss, injury or stealth of communication, mailing or data travelers on open channels;
- Using calendar or event processing systems, moreover creating a scope of activity of supervising for exploring system problems or unauthorized admissions or admission tries.

I stated that there are no essential differences in the usable security solutions of information systems of public administration or for profit sector, but their usage in the information systems of public administration is less prevalent. That is why the implementation of the above mentioned solutions is necessary, with their usage the security of the information systems of public administration can be developed significantly.

Thesis

1. By creating the functional and structural model of the information systems of public administration and by analyzing their working processes, security regulators I explored their lacks, I presented the directions of development and I stated the requirements of the creatable information security strategy in these organizations, the possible build-up of the strategy and the tasks of the information security politics connecting to the previous issues.
2. Based on the structured model of the information systems of public administration I analyzed the attackers against them and the types of attacks, and as a result I created a new categorization of the threats (attackers) against these systems.
3. By observing the attackers and the types of attacks and by analyzing statistically the rate of targets moreover by my own testing results I compared the most used operation systems in the information systems of public administration in the aspect of secure utilizing and I certified that using close operation system is not more disadvantageous than change to open-source operation systems which are more commonly showed as targets.
4. Based on the purposed, particular risk and effect analysis concentrated on the threats and defense lacks I observed and valued the modern information security solutions and as a result I suggested their adaptability in the information systems of public administration, with these the information security of organizations in the civil service sector could be developed effective.

Recommendations

1. I recommend the chapter of my PhD essay about regulating the safety of the information systems for the public administration for making new law intent to develop the defense of the information systems of the public administration for a higher level, and to implement the recommendations to the information security strategy of the organizations.

2. I recommend the utilization of my essay in the bachelor, masters and PhD curriculum of the higher education teaching students on the field of information technology of the public administration.

3. I also recommend the chapter dealing with the forms of attacks of the information systems and the applicable defense solutions for the bachelor, masters and PhD curriculum of the higher education teaching students on the field of information security.

List of publications

Articles in vetted periodical

1. V. Póserné Oláh: *Security and performance of the webservers in the open source and the closed source operation systems*, Scientific Bulletin of "Politechnika" University of Timisoara, Romania, Vol. 55(69), No. 1 / March 2010, pp. 43-48., ISSN 1224-600X
2. V. O. Póserné - Zs. Haig: *The Forms and Defence Possibilities of the Threats Against Computer Networks*, Hadmérnök, 2006. I. évf. 1. sz., Budapest, 2006, p. 13, ISSN 1788-1919
3. V. O. Póserné: *The security of Web Applications*, AARMS Vol. 8, No. 1, 2009, pp. 173-178., ISSN 1788-0017 (Online), ISSN 1588-8789 (Print)
4. Póserné O. V.: *Az információs társadalom és a terrorizmus kapcsolata*, Bolyai Szemle, 2006. 1. sz., Budapest, 2006, pp. 145-159., ISSN 1416-1443.
5. Póserné O. V.: *IT kockázatok elemzésük, kezelésük*, Hadmérnök, 2007. I. évf. 3. sz., Budapest, 2007, p. 9, ISSN 1788-1919
6. Póserné O. V.: *A szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételei*, Hadmérnök, 2007. I. évf. 4. sz., Budapest, 2007, p. 10, ISSN 1788-1919
7. Póserné O. V.: *Rejtjelző módszerek vizsgálata*, Hadtudományi Szemle, 2008. I. évf. 1. sz., Budapest, 2008, p. 14, HU ISSN 2060-0437
8. Póserné O. V.: *Nyílt és zárt forráskódú operációs rendszerek leggyakoribb szolgáltatásainak vizsgálata biztonság és teljesítmény szempontjából*, Bolyai Szemle, 2009. XVIII. évf. 4. sz., Budapest, 2009, pp. 103-117, ISSN 1416-1443

Discourses appeared in conference issues

1. V. O. Póserné: *Comparing the webservers of the opensource and the closed source operation systems*, Proc of the 5th International Symposium on Applied Computational Intelligence and Informatics, Timisoara, Romania, IEEE Catalog Number CFP0945C-CDR, ISBN 978-1-4244-4478-6, Library of Congress 2009903350, 2009, pp. 169-172.
2. Póserné O. V.: *Az Internet adta hadászati lehetőségek és veszélyek*, Robothadviselés 4.

nemzetközi tudományos konferencia kiadványa, Budapest, 2005, pp. 136-148., ISBN 963 7060 08 1

3. Póserné O. V.: *Informatikai biztonság gyakorlatban*, Matematika-, fizika, számítástechnika főiskolai oktatók XXX. konferencia publikációs kiadvány-CD, Pécs, 2006, p. 5, ISBN-13: 978-963-7298-12-7
4. Póserné O. V. - Katona K. - Szénási S.: *A Delphi haladó eszközeinek alkalmazása*, Matematika-, fizika, számítástechnika főiskolai oktatók XXX. konferencia publikációs kiadvány-CD, Pécs, 2006, p. 6, ISBN-13: 978-963-7298-12-7
5. Póserné O. V.: *Számítógép-hálózati támadások*, Hadmérnök, Robothadviselés 6. tudományos szakmai konferencia Különszám, Budapest, 2006, p. 9, ISSN 1788-1919
6. Póserné O. V.: *A távoli munkavégzés biztonsági kérdései*, Hadmérnök, Robothadviselés 7. tudományos szakmai konferencia Különszám, Budapest, 2007, p. 9, ISSN 1788-1919
7. Póserné O. V.: *A kapcsolók hatása a hálózati biztonságra*, Informatika Korszerű Technikái Konferencia 2008, Dunaújváros, 2008, pp. 102-109., ISBN 978-963-87780-2-4
8. Póserné O. V. – Schubert T.: *Informatikai biztonság – szakirányú képzés a Budapesti Műszaki Főiskolán*, Informatika a felsőoktatásban 2008 konferencia publikációs kiadvány-CD, Debrecen, 2008, p. 8, ISBN 978-963-473-129-0
9. Póserné O. V.: *A magyar közigazgatás az informatikai biztonság szemszögéből*, Bolyai Szemle, 2008. XVII. évf. 4. sz., A Robothadviselés 8. Tudományos konferencia előadásainak szerkesztett változata, Budapest, 2008, pp. 157-166., ISSN 1416-1443

Curriculum vitae

Private dates:

Name: Valéria Póserné Oláh

Date of birth: 20.03.1962.

Address: 2030 Érd, Takács str. 5.

Phone: +36-70-604-3007

E-mail: poserne.valeria@nik.uni-obuda.hu

Education:

Zrínyi Miklós National Defense University, correspondence (part time) PhD Training

1991 - 1994: Kossuth Lajos University, Information technology teacher

1982 - 1985: Kossuth Lajos University, Programmer

Language knowledge:

English: intermediate, professional complex „C”

Russian: basic, equivalent with basic „C”

Information technologies knowledge:

Assembly languages: C#, Delphi, Pascal, HTML, Basic, PL1

Operation Systems: Windows Server 2003/2008, Novell, Linux, Windows 9x/2000/XP/Vista/ Windows 7, Windows NT Workstation, MS DOS

Other: IBM Tivoli Identity Manager, IBM Tivoli Directory Integrator, HP WebInspect, IBM Rational AppScan, PGP, OpenSSH, Access, Word, Excel, PowerPoint

Employments:

2004 - Óbuda University, Budapest, assistant professor

2007 - 2010 College of Dunaújváros, Dunaújváros, assistant professor

1995 - 2004 Szent István University VTI, Budapest, assistant lecturer, head of computer laboratories

1987 - 1995 Csiha Győző Secondary School, Hajdúnánás, teacher of mathematics and Information Technology

1985 - 1987 Üvegipari Művek, Orosháza, programmer

Scientific, social organization membership:

2008 - NJSZT membership

Budapest, 22. June 2011.

Valéria Póserné Oláh