Microsoft Technology as an Optimization Tool in Promoting Security and Functionality of the Educational System

Jelena Jardas Antonić[1], Danijel Antonić[2]
[1] Faculty of Economics Rijeka, Rijeka, Croatia
[2] City of Rijeka, Information technology institute, Rijeka, Croatia

***Abstract*—In the cooperation with the City of Rijeka, the project of analysis of the functional and security situation of information infrastructure has been initiated in 24 schools in the authority of the city. Having completed the multicriteria analysis of the collected data, we have built a model of implementing Microsoft service technologies. The implementation should satisfy the elementary security principles that are required by the security standards today, maximizing functionality of infrastructure and minimizing network administration tasks. Server technology that has been used in this solution is Microsoft Widows 2003 Server R2 and Internet Security and Acceleration Server 2006, as well as the GFI WebMonitor and antivirus.**

Index Terms—Microsoft technology; optimization tool; security and functionality of educational system

I. INTRODUCTION

Implementation of information technology in primary school education is imperative today. It follows the digital revolution era. However, if implemented unsystematically and without coordination with today's security standards, it represents a great security risk for the schoolchildren and the administrative load, and an additional cost for the school. This article springs from the need to analyze the current situation and to choose the best solution that will raise the level of security, and cut down maintenance costs.

The project has been initiated by the City of Rijeka, a co-owner of 24 primary schools. This text will, not only present the collected data and the recognized problems, but it will also provide an optimal solution.

II. DESCRIPTION OF THE CURRENT SITUATION

A. Infrastructure

The current situation on the subject of informatization in primary schools can be described as averagely satisfactory. The number of computers varies between schools, and the number of schoolchildren and the school size are not always proportional to the number of computers owned by the school.

The analysis of the situation has also shown that, in regard of location, computers can be divided in several groups: those in information science demonstration rooms, other classrooms and in the offices (the accounting department, the secretary's office and the headmaster's office).

As far as technological level is concerned, it also varies depending on particular schools, the supplier and the time of supply, but, generally, the infrastructure is dominated by computers equipped with Windows XP operation system. However, this domination in 79% of cases does not provide the real picture, since the computers have uneven performances, and some of them are barely usable.

B. The Network

All the computers in the information science demonstration rooms are in the LAN network and none of the schools owns a centralized IT resources management, a domain, etc. Internet access is established by Carnet optical connection in most schools. In schools without a built optical infrastructure, Internet is accessed by ADSL or ISDN connection.

Frequently, there are both connections and, in some cases, more than one ISDN connection, which results in unnecessary costs. As often as not, schools do not use the resources at their disposal, due to lack of knowledge related to launching them or to lack of network infrastructure. Lack of connection with the information science demonstration room has made it possible for a certain number of schools with optical connection to have separate Internet access. This is good in terms of security, although it is not optimal in regard of costs and performances required by the Ministry programs for school resources record keeping (eRegister or "e-Matica" in Croatian).

In schools with optical connection, one LAN frequently hosts office workers' computers and information science demonstration room computers without network segmentation, which is a great security oversight. It is unallowable for the headmaster's computer, as well as computers in the accounting department and the secretary's office, to be freely accessed from computers in the information science demonstration room. Three schools are using a wireless connection, but none of them has access protection.

Security situation in schools is diverse. There are schools without antivirus protection, schools which purchased antivirus software and those that use some of the free antivirus software, whose quality is far behind the commercial tools. All of this results in the fact that the computers are infected by viruses. Thus, computers break down more frequently, which requires greater teacher's engagement. There is also a rise in the possibility of pornographic content appearance and infection of children's home computers, as well as computers in the

offices, since the networks are not segmented. Only 25% of schools have a segmented network and access restriction. **Not a single school has a pornographic and hazardous content filter.**

C. Hardware maintenance and computer management

Hardware problems with the equipment have been solved in different ways. In some schools, commercial companies for supply and replacement of faulty components have been hired, while in others information science teachers obtain the components and replace them by themselves.

Computer management is the most frequently mentioned problem of information science teachers. Accordingly, teachers dedicate a great amount of time to computers maintenance, virus deletion (in schools with AV protection) and reinstalling operation systems and software needed for teaching and for administrative work. This, of course, is not their job, and they should use this time to prepare their lessons. This is the reason why 84% of teachers complain about enormous time consumption related to maintenance of computer infrastructure (repairs, reinstallations, failures) needed for teaching, as well as for school administrative work.

After the collection of data in 24 primary schools, these schools were ranked with the aid of Expert Choice software package and AHP method [3]. They were ranked as regards their current situation and the criteria chosen as essential Criteria that have been used for AHP data analysis are number of computers, number of techers of informatics, conection on internet, ativirus programs, net segmentation, etc. Weighing the importance of particular criteria and their coupling resulted in the final order of schools (Picture 1). Subsequently, schools that are most suitable for the project have been chosen for the pilot-project.

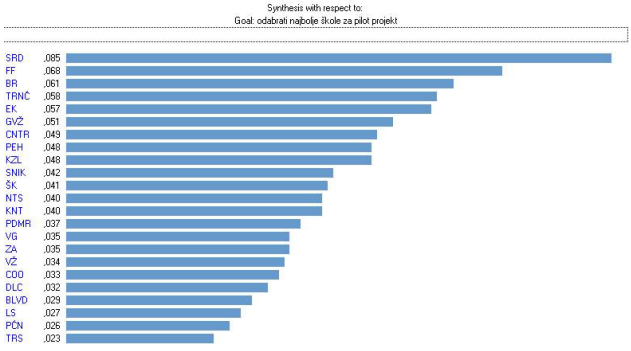

Figure 1. Results of the AHP data analysis

III. SOLUTION TO THE PROBLEM

While creating the solutions to the problem of optimization of network infrastructure, the research team had to bear in mind the fact that the City of Rijeka wanted to provide schools with full autonomy of information system. At the same time, the City wanted to have constant insight into the state of the system and collection of data in real time. Since this is a complicated implementation, the idea of starting a pilot-project with several schools emerged. In order for the server technology to be integrated with the school infrastructure more easily, these schools should already have educated employees. A system engineer would control server operation and be at disposal in case of system failure. As one of the goals is to use new implemented technology to the maximum, the need to familiarize the teacher staff with the system possibilities emerged, as well. This will reduce their involvement in computer infrastructure maintenance, i.e. the amount of their administrative tasks, while system efficiency will rise.

Since every primary school is entitled to Microsoft server products, under the cooperation agreement between the Ministry of Science, Education and Sports and the Microsoft Company, the optimal solution was to implement a Windows Server 2003 R2. Although Linux servers were under consideration, it was evident that they lack the possibility of centralized administration of Windows client computers. Therefore, Microsoft security technology was chosen as the best solution, since it provides centralized and effective sharing and management of the information coming from the network resources and the users.

In order to enhance the level of security within the network, we came to the conclusion that the users rights in regard of changing the user interface, installing applications and access to the network resources, should be in accordance with their role in the education process and the hierarchical school structure, which was not the case earlier. The restriction will be implemented by the Group Policy and NTFS right for the file system [2]. Group Policy will render intentional or accidental change of the computer interface display impossible, as well as installation of unallowed software. Finally, this should result in more stable computer operation, a higher level of security with a lesser possibility of catching infections with malicious software (viruses, spyware). Consequently, the need for regular computer repairs would be reduced. Group Policy would also enable installation of applications on all computers in school or on a particular group of them [5]. This kind of distribution would provide simpler and faster software installation, and its control. Group Policy flexibility, which allocates an application to the user or to a computer without the need for his or her interaction during the installation process, enables the application to “follow” the users regardless of the fact which computer they are using at the moment. These privileges will mostly be used for teacher staff. In addition to all this, centralized deinstallation of applications will be made possible. We stated only some of the favourable conditions, which will reduce the need for administration of each computer.

Active Directory use on the main server will create groups with the associated rights for computer usage and for access to the network resources (Picture 2.). Groups will be created depending on which user group the user belongs to (professors, administrative workers, the 8th grade, the 7th grade…) AD service server would also contain the centralized base of user accounts which would make it possible for the teachers and schoolchildren to log in with their user name and password on any computer that they are allowed to use [6].

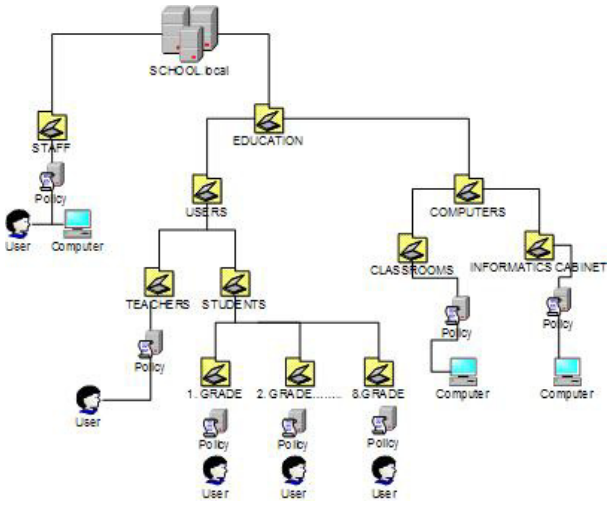

Figure 2. Active Directory design and group policy implementation

The offered solution makes it possible for the documents of each user to be accessible regardless of the computer he or she is registered at, since the user profile settings will contain redirection of register maps to the central server. This kind of implementation enables easier creation of safety copies of private user data, due to the fact that the important user data are on the server and that safety copies are backed up on a weekly basis. However, this kind of implementation brings along the danger of overloading the server with irrelevant user data. The stated problem will be solved by using disc quotas that will limit the amount of space on the server allocated to each user, depending on the group that the user belongs to (schoolchild, professor…). This solution will also provide control over any unauthorized attempt of computer registration or access to unallowed resources on the network [4].

Saving unwanted file types on the server by the schoolchildren, such as songs or movies, will be prevented with File Server 2003 R2 advanced filter options .

Implementation of the patches will be centralized and done by WSUS (Windows Server Update Services), which enables automatic patches upgrade on the computers with the Windows operation system.

Every teacher will be able to connect to the school server from home by VPN (Virtual Private Network), and have access to his or her documents on the server, used, for example, for lesson preparation.

The antivirus solution was initially imagined in a client-server variant of an antivirus commercial tool, which would be an optimal solution with regard to very good characteristics in virus detection that these tools have. However, due to the fact that the Ministry of Science, Education and Sports is currently in the phase of obtaining the antivirus solution for all primary schools in Croatia, we decided to choose the Avast antivirus tool. In accordance with this, the chosen anti-spyware solution is Spybot Search and Destroy, which is also a free tool.

We presume that, in the initial phase of implementation, the choice of the free solution is a satisfying option, since malicious code cannot harm the software significantly, due to the fact that all user accounts have restricted user rights. This means that even the virus that enters the computer cannot harm it significantly.

Network segmentation, as an indispensable factor in securing the network infrastructure, will be done with one of the best tools today, Microsoft Internet Security and Acceleration (ISA) Server 2006 (Picture 3.). The network will be segmented in three parts: computers in the information science demonstration room, classrooms and offices (classrooms include computers the teachers use for teaching in the classrooms). All three segments would have access to Internet, while communication within the network would be one-way; from the classroom to the information science demonstration room, but not vice versa. Communication on the Internet would be restricted only to particular services (HTTP, HTTPS, SMTP, POP), which would prevent Peer to Peer tools and other applications to release information from the school network without authorization [1]. ISA Server 2006 would be the firewall and the proxy server. The firewall works on all 7 layers of OSI Presentation, which renders an in-depth analysis of the Internet protocol, such as Hypertext Transfer Protocol (HTTP) possible, and detects many threats that the traditional protection walls cannot detect.

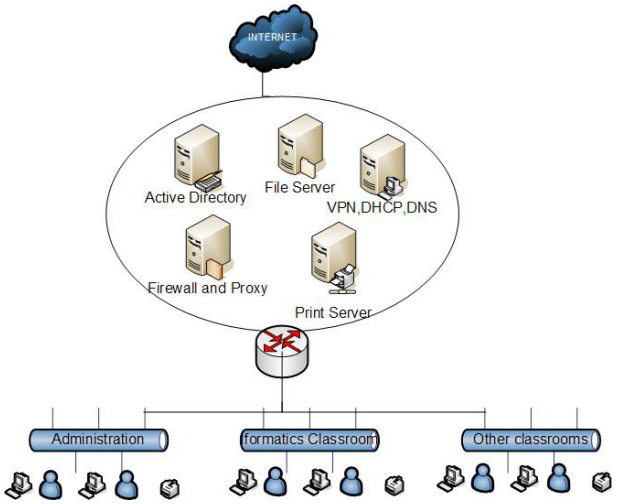

Figure 3. Network segmentation and design

The possibility of an in-depth analysis of the packages sent to the school network from the Internet, enables stopping the packages that contain files whose downloading on the local network had been prohibited. The lack of possibility of downloading the EXE, RAR and ZIP software on local computers is a great step in the fight against viruses, while prohibiting film downloads prevents unnecessary overload of the school network resources. Proxy function of the ISA Server enables faster work on the Internet due to the fact that the content the teacher displays on his or her computer while teaching is saved on the ISA Server at the same time, so the schoolchildren who repeat the action after the teacher can read the content from the local server, which accelerates work if the school has a slower Internet connection. Integration of the ISA Server with the GFI WebMonitor tool, which was used only in the trial version of this test implementation, enables control of the Internet content even before it reaches the client computer with three antivirus tools, which is a terrific option. The GFI tool offers a possibility of controlling the content that the schoolchild is downloading as regards his or her age, since we can filter the web pages which contain violence, pornography… Every school system should have this type of a filter since

the children are exposed to a huge amount of pornography on the Internet today.

All these tools represent a base that every school system should have to gain functionality and usefulness the information technology is intended for. However, this base should be upgraded and developed continually in order to prevent the situation we find in schools today from happening again.

IV. CONCLUSION

After analysis that has been done, it can be concluded that all used tools in the paper represent a base for every school system if we want to achieve high level of functionality and utility which must exist for that kind of informatical technology. Informatical system implemented in this way, should be permanently built and developed for remain on this level of security and not be recovered. Development of the informatical infrastructure without staff education, with the accent on the principles and the teachers of informatics, wouldn't brigs us success we expect in use. Principal who do not understand functionality importance of the informatical infrastructure wouldn't know how to motivate disinterested school staff, and on the other way he could stop any positive initiative. Solution offered in this paper it is not the best solution which we can get using commercial tools, but we can say that is the closest to the best commercial solutions respecting the existing financial constraints we had as an obstacle for it's implementation.

REFERENCES

[1] Tom Shinder, *Configuring ISA Server 2004*, 2nd Edition, Syngress, 2004.

[2] Sakari Kouti and Mika Seitsonen, *Inside Active Directory: A System Administrator's Guide*, 2nd Edition, Addison-Wesley, 2004

[3] Thomas L. Satty,*Fundamentals of Decision Making and Priority Theory*, 2nd Edition, RWS Publications, 2006.

[4] Microsoft Official Course: Implementing and Administering Microsoft® Windows® 2000 Directory Services, Microsoft Press ©, 2002.

[5] Jill Spealman, Kurt Hudson and Melissa Craft, *Planning, Implementing and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure*, Microsoft Press ©, 2004.

[6] Robbie Allen, Alistair G. Lowe-Norris ,*Active Directory*, 2nd Edition, O'Reilly, 2003.

AUTHORS

J. Jardas Antonić is with the Faculty of Economics Rijeka, Department of Quantitative Economy, 51000 Rijeka, Croatia (e-mail: jjardas@gmail.com).

D. Antonić, is with City of Rijeka, Information technology institute, 51000 Rijeka, Croatia (e-mail: danijel.antonic@rijeka.hr).

This article was modified from a presentation at the 31st International Convention MIPRO 2008 in Opatija, Croatia, May 2008. 2008). Manuscript received 07 August 2008. Published as submitted by the authors.