SECURITY POLICY IN WINDOWS OPERATING SYSTEMS: E-LEARNING

Jakub SELIGA, František ADAMČÍK, Jozef GALANDA*, Radoslav ŠULEJ
Faculty of Aeronautics, Technical University Košice, Rampova 7, 041 21 Kosice
Martin JEZNÝ
Letisko Košice – Airport Kosice, a.s., Letisko Košice, 041 75 Košice
**Corresponding author*. E-mail: jozef.galanda@tuke.sk

Summary. This article informs reader about security policy in Windows operating systems in terms of defining, setting up and using their security policies. The authors analyze, in the field of security of Windows 7, the security features in the new operating systems Windows 8 and 10 considering their mutual differences, advantages and disadvantages. Article contains a proposal of e-learning course. The proposal is processed with respect to new trends in this area.

Keywords: Security policy; Windows 7; Windows 8; Windows 10; E- learning; Moodle

1. INTRODUCTION

In today's information age when electronic data is necessary to protect and to ensure the device, therefore, the people responsible for the management and operation of systems is expected to set the appropriate measures to strive remove the incidence and consequences of negative effect. The security policy is a set of rules and resolutions that can be defined permitted and non- permitted actions of users and possible countermeasures to them. It describes the safety objectives and sets out the principles of the protection process, restrictions, requirements, rules and procedures, which specify the methods of protection, administration and handling of files and folders box.

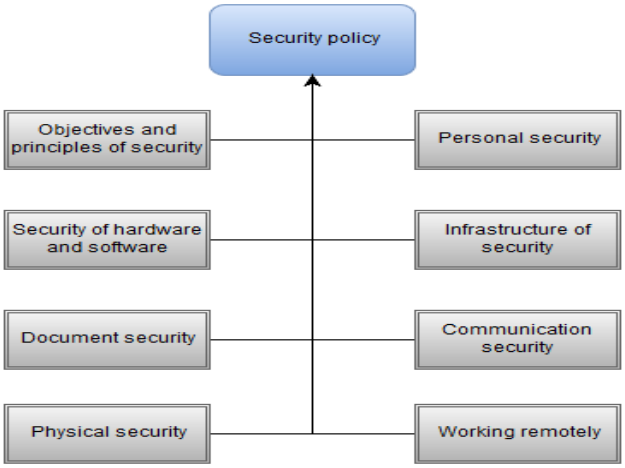

Figure 1 Content of Security Policy

2. SECURITY POLICY IN WINDOWS 7

Security policies are rules which administrator to configure one or more computers in order to protect computer or network. Security Settings allows you to define security configuration by the GPO (Group Policy Objects). These are linked with the directory components of the Active Directory domain, etc. and allows administrators to administer security settings for multiple PCs from any computer connected

to the domain. The security settings can manage user authentication, either on the network or computer which users have access and whether to record the activities of users or groups and group membership. Furthermore, adjustment policies allow you to control the configuration of the operating system and its components. It is also used to configure the computer user scripts, folder redirection, your system and installing the software [5].

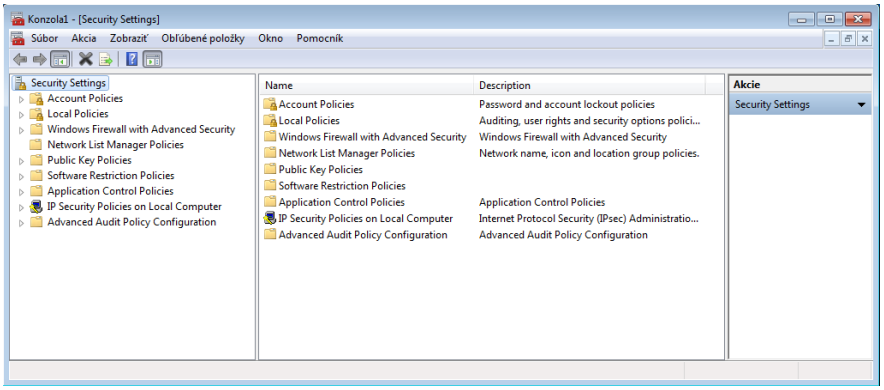

Figure 2 Security policies in OS Windows 7

Individual workstations in the computer network can be configured locally if the configured computers are members of the work group or home group, as well as domain members. On the local workstation can be local security and user access to system configured only if the computer is a member of the work group. If the computer is a domain member, security and user access can be configured on two levels: on local system level or on domain level. On the domain level can be access specified through directory services of Microsoft Active Directory.

Individuals can use for logging so-called user accounts. Group accounts are used to facilitate the management of multiple users. User can login to system only through user account, not through group accounts. Each user account is identified in the operating system via the so-called SID (Security Identifier). SID is unique and unalterable identifier of user or user group. Operating system generates a SID that identifies a particular account or group at the time the account or group was created. Generated ID can never be reused to identify another user or group what was created. There are also well-known SIDs that identify the general group and ordinary users. For example, the Everyone SID identifies a group that includes all users of the system. Known SIDs have a values that remain constant across all operating systems (such as SID for the user, administrator, domain, etc.) [6].

Group Policy is a tool with which we can manage rights and privileges applicable to the entire workstation as well as logged in users. Group Policy allows us to create complex settings, which are called Group Policy object (GPO) that can modify the parameters of computer behavior or user behavior. By using Group Policy the administrator can manage the configuration of the operating system as well as enable or disable capabilities and user interface controls. All Group Policy settings are stored in the registry of operation system. Computer configuration is in the "HKEY_LOCAL_MACHINE", user configuration is in "HKEY_CURRENT_USER". Group Policy simplifies administration, because administrators can centrally set permissions and options for users and computers. For the proper functioning of the system is a prerequisite thorough management of policies. These are divided into two categories as settings related to computer and settings for users. On starting the operating system generally apply that computer policy and user policy are applied after logging user [1] [2].

During configuration policies under the "Computer Configuration" and "User Configuration" we find the same nodes that depend on the options installed and what kind of policy we use. In both configurations are typically contains the following child nodes:

- Setup software – It is the policy settings for configuring and installing software
- Windows settings – Policy setting to redirect folders, textbooks and security
- Administrative Templates – Policy settings for the operating system, Windows components and programs.

If we want to manage a user or computer, we must configure a policy to manage the so-called templates. This policy provides easy access to the settings registry-based policy that controls the operating system, Windows components and programs.

Previous versions of Windows to provide the function of Group Policy to store that policy-based registry to file administrative template (ADM) in its specific markup language, but Windows 7 uses a standard file format based on XML language called AMDX. Compared ADM files that are loaded in the associated GPO and ADMX files are placed in a central repository on Domain Controller Server.

The security policy settings are rules that administrators configure on a computer or more computers In order to achieve protection of resources on your computer or network. These settings features in Windows help secure system of against potential threats. Here are the following features such as (see Figure 2):

- Accounts policies that determine how user accounts can interact. These include password policy and account lockout policy, see Figure 3).
- Local policies such as audit policy (event logging), assign user rights to users or groups, computer security options, see Figure 3.
- Windows Firewall with advanced security
- Network list manager policies
- Public Key Policies (Encrypted File System management, BitLocker Drive Encryption, etc.),
- Software restrictions policy
- Application Control policies
- IP security policies on Local computer

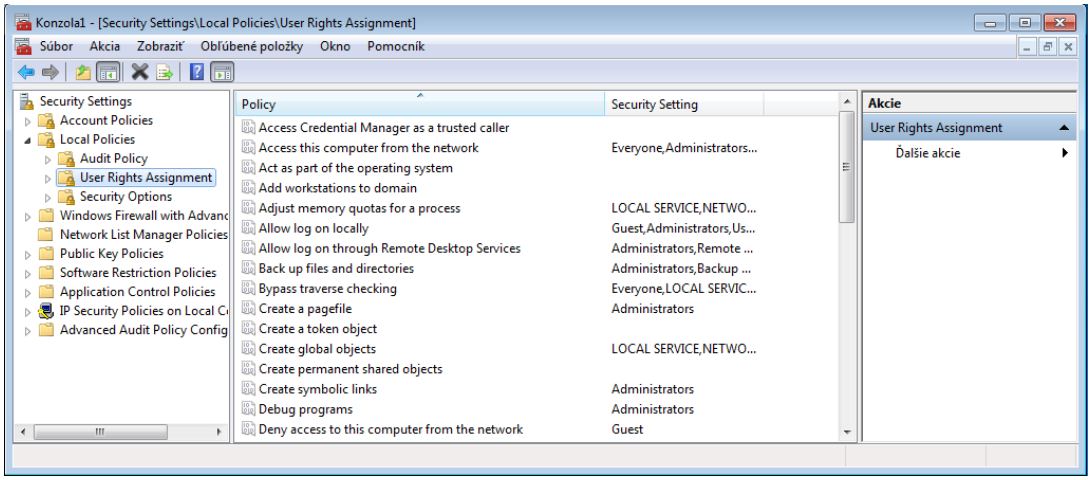

Figure 3 User Rights Policies in OS Windows 7

All the most important security settings of devices running Windows especially in security accounts, local security and network security are with greater or lesser changes applied in the latest versions of Windows, such as versions 8 and 10.

3. SECURITY IN OPERATING SYSTEMS WINDOWS 8 AND WINDOWS 10

Microsoft gives more emphasis on safety of operating systems Windows 8 and Windows 10, which introduces new elements to ensure that devices with these operating systems. Besides to already common setting security policies, user groups or networks, Microsoft is committed to the integrity and safety of the equipment in the following areas [3]:

Identity and access control

Features have been greatly expanded to both simplify and enhance the security of user authentication. These features include Windows Hello and Microsoft Passport, which better protect user identities

through easy-to-deploy and easy-to-use multifactor authentication (MFA). Another new feature is Credential Guard, which uses virtualization-based security (VBS) to help protect the Windows authentication subsystems and users' credentials.

Information/Data protection

Functions in this area guard information at rest, in use and in transit. In addition to BitLocker and BitLocker to go for protection of data at rest, Windows 10 includes file-level encryption with Enterprise Data Protection that performs data separation and containment and, when combined with Rights Management services, can keep data encrypted when it leaves the corporate network. Windows 10 can also help keep data secure by using virtual private networks (VPNs) and Internet Protocol Security.

Malware resistance

This area includes architectural changes that can isolate critical system and security components from threats. Several new features in Windows 10 help reduce the threat of malware, including VBS, Device Guard, Microsoft Edge and an entirely new version of Windows Defender. In addition, the many antimalware features from the Windows 8.1 operating system— including AppContainers for application sandboxing and numerous boot-protection features, such as Trusted Boot—have been carried forward and improved in Windows 10.

Microsoft in recent years, placing more emphasis on the security of operating systems Windows 8 and to Windows 10 in which introduces new elements for security of devices. In addition to conventional setting security policies of user, group or network, Microsoft puts emphasis on integrity and security to protect data using a set of enhanced features for authorizing, auditing and data encryption without it acted difficulties of users or system administrators. Prevention is the best choice. Windows introduced a strong resistance against attacks taking advantage of secure hardware, using secure boot process and using secured kernel of operating system.

3. ELECTRONIC EDUCATIONAL TECHNOLOGIES

Electronic learning technologies facilitate learning of students and improve the study, practice and performance of students through the creation and using of appropriate technological processes and resources. This includes the use of the hardware, software and educational theory of course. There are several aspects that describe the intellectual and technical development of educational technologies:

- educational technology as a theory and practice of educational approaches to teaching
- educational technology as a variety of technological tools and media to help in communication and to development and exchange of knowledge
- educational technology for learning management system, such as tools for students, curriculum management and management information systems education
- educational technology as an educational subject; These courses can be called "Computer Studies" and "Information and Communication Technologies" [7]

Distance learning can be understood as learning from any distance, where major part of students is physically away from the teacher. It's actually attendance, where the student must be physically present in the activities. Such studies do not consider as distance learning. This is a planned teaching, supervised by the teacher. If someone decides to study by distance form it needs to be sufficiently motivated and was able to schedule their study time. In the past, distance education carried out by regular mail and written communication between teacher and student. Nowadays, term distance learning means a specific distance learning system, which is based on the use of modern information technologies. It is a modern electronic communication between trainees

Distance learning offers many advantages for the students and for the teacher or educational institution. Among the most important are:

1. Students can customize their time, space and learning process. We find out that by this form of education student is better able to apply knowledge to real life. They responsible for himself and for his performances and this is the main motivation for such a way of life. Therefore, we think it preferable to personally advanced students or working people who are educated part-time.
2. It offers free access to teaching for students. The advantage is that the students of this form of learning can happen to anyone regardless of residence of the student and the university. Distance form is easier to study the technical and humanities due to the possibility of re-reading of the issue.
3. Training materials are edited in easily understood and it provides easy understanding of the student curriculum.
4. From an economic perspective it will reduce the financial cost of the study (travel, accommodation, meals ...) and by the institution of the elimination of operating costs (classrooms, equipment, light, heat ...)

As an additional advantage we can consider involvement of the students in the educational process, student's self-reflection and their stress relief (especially in testing). As an additional disadvantages we can consider that teachers must process study material in the highest quality, students lose social contacts, become isolated and lose motivation to go ahead with the study. An examination of students' knowledge is difficult because for teachers is difficult to find out whether the student works independently or not [4].

3. THE COURSE

The proposed course is intended for students and students of Faculty of Aeronautics. It is processed at a professional and acceptable level within university studies at the Faculty of Aeronautics. The course has been divided into several themes have been focused on the issue of security, security policy, setting and securing Windows 7 operating system and subsequently operating systems Windows 8 and Windows 10. Themes we created to the form of active lectures, which ends with one sometimes two control question for which a student has the opportunity to get plus points of passing the exam. Questions are based on theory and exercises included in course. Complex lectures are divided into "sub lectures" describing the specific question at a more detailed level.

Structure of the course

Planned course we processed into several themes. Each theme is dedicated to a specific field of security policy of Windows OS. All information is processed to the form of lectures and exercises. For example the objective of the first theme is to manage knowledge on definitions of safety policies, their content, structure and subsequent application in Windows operating systems. After studying of this theme students should be on the basis of that information able to manage discern the suitability of applying specific policies. This lecture describes general security policy of operating systems and how it is divided. Another part of this lecture provides an introduction to the topic of security policies on Windows 7. Table 1 show the complex structure of lecture.

Table 1 Lecture number 1

Name of the page	Type of the page	Action
Introduction	Table with branches	End of lectureNext page

Types of security policies	Table with branches	End of lecture Next page Previous page
Security Policy in Windows	Table with branches	End of lecture Next page Previous page
Security Policy in Windows 7	Table with branches	End of lecture Next page Previous page
Versions of OS Win 7	Table with branches	End of lecture Next page (end)

The second topic explains to students the issue of user accounts and groups on Windows. We are dealing here mainly clarifying the accounts as an administrator and guest who are often subject to misconceptions about their application of the system. After completing the theoretical knowledge of the topic the student should distinguish between accounts and avoid their misuse. Objective of the third theme is the comprehensive analysis of the issue of security policies, how they affect user accounts on the system and data security. The result is a system of setting individual safety policies as difficult administrative tasks. Particular sub-themes detailed describe the policy accounts, computer policies, policy groups and network policy. Practical tasks contains methods to setting policies. The Fourth topic describes the new system of enhancements and security policy in Windows 8 and 10. Explains new features and new security tools in Windows 8 and 10 and their differences compared to Windows 7 with respect to the security system from virus attacks, data protection and access control to the computer. The final realization of the course in faculty LMS Moodle you can see on Figure 4 and online at http://www.moodle.leteckafakulta.sk/course/view.php?id=284.

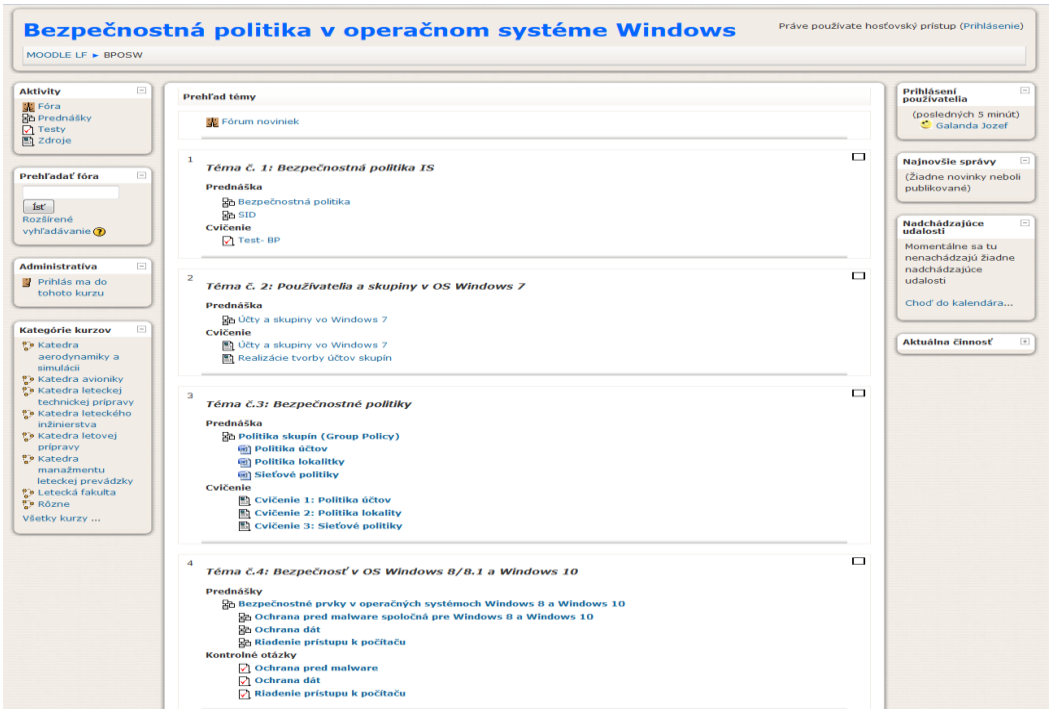

Figure 4 The final course realization

After completing the course the student should master new trends and directions in the development of security of operating systems, development of reliable security policies and be able to configure the operating system so that it is resistant to critical situations in systemic security and protection of

operating system. Quality of the protected operating system is key to the reliable operation and safe running applications.

6. CONCLUSION

With the gradual development of operating systems shall also developed various options for attacks on the operating system. Based on the findings of the comparison level of security, we concluded that the security is rapidly changed from classical architecture of security in Windows 7 to modern system of security architecture in the operating systems Windows 8 respectively 10. This architecture focuses on server-client communications at the time of starting the operating system and therefore can deliver timely protection from attacks and penetration into the system as architecture that was used in previous OS versions. We point out that Windows 10 with these new methods of ensuring becomes paradoxical network operating system. Nowadays, Windows 7 is still the most preferred OS (even though they are already available to its more modern successors) because it is free from defects such as Windows 8 or 10. And so comes along question: What after useful life of Windows 7? Microsoft ended classical support for Windows 7 since January 2015. He provides just extended support, which means only security updates and only until 2020. It would be helpful to wait with transition to newer operating systems until time, when will be fixed all security flaws of Windows 8 and 10. Important is flexibility in decision-making when selecting the Windows operating system, because its content involves comparing the levels of security that are never developed such as one complex in one place.

Theoretical knowledge of various security policies were processed into the present electronic course. The course is designed for students of Faculty of Aeronautics, but can also become a guide to ordinary users of information technology. The course is created in Moodle Faculty of Aeronautics, which is suitable for spacing the way of education. It benefits from various aspects, for saving time, space and costs, whether on the part of the student or educational institution. The question arises whether these benefits outweigh the social contact that is in this type of study is losing. We highlight that universities adapt to using e-learning. Currently, electronics and computer learning tools are adapted to this trend. But many universities still consider e-learning methods only as a supplement of face to face teaching.

ACKNOWLEDGMENT

This work was supported by the Slovak Research and Development Agency under the contract No. APVV-15-0527 "New generation of departure control system for an airports".

References

Books:

[1] Stanek, W. R. *Microsoft Windows 7: Kapesní rádce administrátora.* First Edition. Brno: Computer press. 2010. 712 p. ISBN: 978-80-251-2792-6

[2] Stanek, W. R. *Group Policy: zásady skupiny ve Windows: Kapesní rádce administrátora.* First Edition. Brno: Computer press. 2010. 352 p. ISBN: 978-80-251-2920-3

[3] Bott, E. *Introducing Windows 10 for IT Professionals, Technical Overview*. First Edition. Redmond Washington: Microsoft Press. 2016. 202 p. ISBN: 978-0-7356-9697-6

[4]. Gazdíková, V: *Základy dištančného elektronického vzdelávania*. First Edition. Trnava: PdF TU. 2003. 64 p. ISBN 80-89074-67-7

Web sites:

[5]. *Microsoft TechNet: Security Policy Settings Overview*. Redmond Washington: Microsoft Press. 2012. Available at: https://technet.microsoft.com/cs-cz/library/hh831424.aspx

[6] *Microsoft TechNet: Security Identifiers.* Redmond Washington: Microsoft Press. 2016. Available at: https://msdn.microsoft.com/enus/library/windows/desktop/aa379571(v=vs.85).aspx

[7] Robinson, R. - Molenda, M. – Rezabek L. *Facilitating Learning.* New York: Routlenge Taylor & Francis Group. 2008. Available at: http://samples.sainsburysebooks.co.uk/9781136503276_sample_494167.pdf