ACTA TECHNICA CORVINIENSIS
– Bulletin of Engineering
Tome IX [2016] , Fascicule 2 [April – June]
ISSN: 2067 – 3809

[1.] László GÖCS, [2.] Zsolt Csaba JOHANYÁK, [3.] Péter András AGG

PROTECTION OF COMPUTER LABORATORIES IN EDUCATIONAL INSTITUTIONS

[1-3.] Department of Information Technology, Faculty of Mechanical Engineering and Automation,
Kecskemét College, HUNGARY

Abstract: There are several technologies and methods for the security related design, management and maintenance of computer laboratories of educational institutions. In order to ensure the continuous availability and the proper maintainability it is crucial to protect the operating systems of the workstations as well as the whole network against internal and external attacks. Thus some kind of control and limitation of the internet based communication and network usage becomes inevitable. Besides, a well-structured, transparent, and secure system management can be obtained only through a central management approach. In this paper, we present some best practice methods and options applicable in case of computer laboratories; and thereafter we examine the current situation by analyzing the results of a comprehensive survey conducted in secondary schools of Kecskemét.

Keywords: IT security, computer laboratory, operating system protection, domain control, firewall

INTRODUCTION

Recently risk factors of computer laboratories of educational institutions have increased owing to the development of information technology and infrastructure [16]. A secondary school is a typical place where workstations, the interconnecting network, and other devices are exposed continuously to several threats. On a large scale, risks can be traced back to the students' malicious and random actions. However, external threats cannot be excluded either. In such situation it is important to interpret properly the need for protection on different fields of information technology, i.e. not only the hardware security has to be ensured but one should also cope with network communication and data security issues, as well as the vulnerabilities of the operating system have to be taken care of. Thus protection should be a priority in order to ensure the easy maintainability as well as the continuous availability of the workstations and the connected services.

There are several methods aiming the assessment of security risks, the reduction of the vulnerabilities resulting from configuration and management errors, and the avoidance of the possibilities of computer attacks. Cost is always an important factor that influences the procurement of tools and devices as well as the selection of applicable methods, especially in secondary schools. However, there are other aspects of security like the short and long time effects of a successful harmful activity that should be also taken into consideration before a decision. Besides, even when someone has a reduced budget there are always low-cost or even no-cost entry level options like introduction of a security focused attitude, definition of a proper computer laboratory usage policy, etc.

In this paper, we present the results of our research related to the available best practice solutions that could contribute to the implementation of a safe, secure, and well maintainable computer laboratory. In order to get a broader picture of the current situation a survey has been conducted in eleven secondary schools of Kecskemét. In the second part of our paper the results of this survey are analyzed in details.

The rest of this paper is organized as follows. Section 2 introduces the possible components of a multilevel security solution that can be considered as best practice. Section 3 gives a picture on the current situation by analyzing the results of the survey conducted in secondary schools.

COMPONENTS OF THE PROTECTION

Securing the physical access

Securing the physical access to the laboratories could serve as a first step towards the ideal protection level of the laboratories. One can control the group of people entering a lab using possession based authentication like magnetic access cards, smart cards, key-fobs (Figure 1), etc. or knowledge based authentication such as a PIN number reader based solution (Rhodes, 2015)(Access, 2015)(Khosrow-Pour, 2014). The advantage of possession based authentication tools are that they are usually cheap and can be immediately disabled when they are stolen or lost.

Figure 1. Access control key fob (Proximity, 2016)

Access control systems (ACSs) make possible the screening of laboratory usage, easy automatic analysis of logs as well as restricting the access to specified time frames of a day (Bunyitai, 2011). Furthermore, these systems eliminate the need for easily duplicated keys. ACS management rights should be given to system administrators or the teachers supervising the laboratory. The physical access restriction based protection plays an important role in avoiding theft of hardware components like mice and memory chips as well as installation of unauthorized devices.

Protection of the workstations

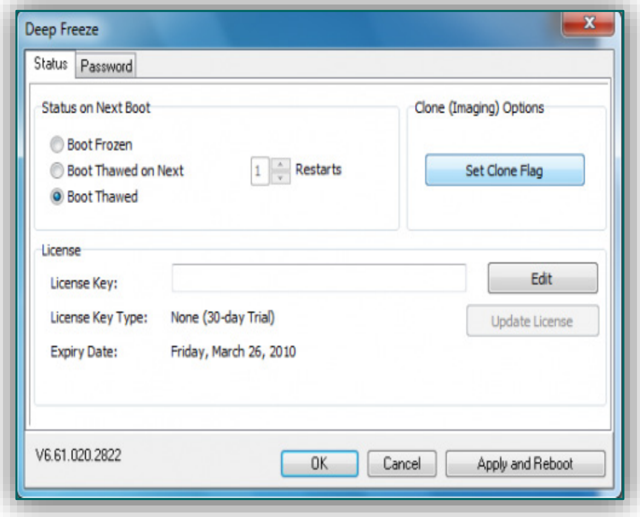
The first and essential step towards securing the workstations of a computer laboratory is the password protection of the Basic Input Output System (BIOS) of the workstations. It is important because this is the place where the boot drive is configured and so it determines from which drive which operating system is started when the computer is switched on. Without a right protection anybody becomes able to modify the boot order and this can led to the possibility of booting from an external drive followed by an attempt on cracking the administrator password on the original system. When the workstation BIOS is protected by a strong password the attacker can be successfully hindered in modifying the BIOS setup. However, this protection can be evaded by removing the battery from the motherboard temporally that leads to the deactivation of the password. Therefore the password protection should be combined with physical protection of the chassis using stickers or more sophisticated tamper-evident technology (Tamper, 2016). Here usually a regular inspection is necessary in order to detect physical attacks against computers.

Figure 2. Tamper evident foil security sticker seals (Tamper, 2016)

Protection of the operating system

It is typical for school computer laboratories that students try to install a lot of applications, and modify the configuration in several ways partly led by curiosity partly thinking that it would make their work more comfortable, and of course malicious misconfiguration attempts are also possible. These activities result in a heterogeneously configured computer group and in slowing down the workstations. Both of these obstruct the effective teaching-learning process and therefore they should be avoided. The first step towards this goal is the proper user/group based sophisticated right and privilege allocation. Students should receive always only those (restricted) rights which are necessary for their learning activity. System configuration abilities should be given only to the staff responsible for system administration.

The only exception to the above mentioned rule is the case when the topic of the subject taught is the system administration itself. In this case an automatic mechanism is necessary, which ensures that after a system administration class everything is brought back to its normal (initial) state. The basic idea is that before starting the semester system administrators create the desired configuration and they define a so called restore point. After finishing the class that resulted in modifications of the configuration everything is returned to the state stored as restore point. It can be done by using the Windows built-in System Restore functionality (What, 2009) or using specialized software like Deep Freeze (Fig. 3) (Deep, 2016). In the first case the restoration effects only the system files and settings and it has to be started manually, while in the case of the second solution after a reboot all changes are removed from the protected partition and the computer is returned to its original "frozen" state. In the latter case the students only need to shut down the computers at the end of each class.



○ Boot Frozen
○ Boot Thawed on Next 1 Restarts
● Boot Thawed

License Key:
License Key Type: None (30-day Trial)
Expiry Date: Friday, March 26, 2010

V6.61.020.2822

Figure 3. Deep Freeze configuration (Deep, 2016)

Centralized system

In case of a big number of users and workstations system administrators are not able any more to manage operating systems, user rights, and data security locally. These tasks can be solved efficiently only by applying some kind of centralized management that helps the simplification and automatization of several recurring tasks. A centralized management always has a hierarchical client-server structure. User accounts and different restrictions, like rules, policies, logon time limits, privileges, etc. are stored in a central database. In case of Windows based systems this database is called Active Directory (AC) (Thomas, 2014) while in case of Linux based systems OpenLDAP (OpenLDAP, 2015) and Samba 4 (Samba, 2016) based solutions are mostly used. Most of the secondary schools have computer laboratories equipped with workstations running Windows operating systems. Therefore, further on we will focus only on Windows based solutions and best practices. In this scenario the server machine hosting and maintaining the central database is called a Domain Controller (DC) and all the computers, which use the AC have to join the domain.

Thus most of the management task done by system administrators has to be carried out on a DC, and also a DC is responsible for the authentication of the users. Tools like Group Policy (GP) make possible for system administrators to control security settings of the operating systems of workstations in a centralized manner configuring it only once and applying it for all concerned machines automatically. For example one can deny all access to removable devices or media with only one GP setting (Thomas, 2014). Similarly one can control the appearance of the Windows Desktop and the availability of different software and Control Panel services as well.

File server and domain based centralized data storage is the key for an easy configurable and maintainable folder access permission system. Besides, it could also be very advantageous for computer laboratories because it facilitates the creation of failsafe storage as well while workstation based user folders can be backed up only in a complicated and more time consuming way. Moreover, if a partition protection based system restore solution is configured on workstations one should put the user folders on a separate partition anyway in order to avoid the deletion of user contents whose persistence is required. Furthermore, the implementation of a systematic backup scheme is also facilitated. The typical backup types are presented below (Backup, 2012).

- Full backup – all the selected files and folders will be backed up.
- Differential backup – all the files and folders that have been modified since the last full backup will be backed up.
- Incremental backup – all the files and folders that have been modified since the last backup will be backed up.

Protected network

Firewalls are standard components of the protection system of an IT infrastructure aiming the prevention of unauthorized access to or from a network. There are hardware, software, and combined implementations for this task. Firewalls control the type of incoming and outgoing traffic by filtering the transmitted data and blocking those data packets that do not meet the specified security criteria (Gattime, 2016). Usually only that incoming traffic is enabled to enter the protected (internal) network which is a response to a query sent from the internal network.

The filter functionality is based on the definition of Access Control Lists (ACLs) that specify which kind of traffic can be enabled or should be denied (CCNA, 2012). An ACL contains at least one command but it can comprise several hundreds of them as well. The commands are executed on the order they were specified. Basically there are three types of ACLs (Configuring, 2007):

- Standard – this is the simplest one, it does the filtering based on source IP address and they are applied to an interface (inbound or outbound).

- Extended – beside the source IP address it takes also into consideration the destination IP address, the protocol, and the port numbers.
- Named – it is a standard or extended ACL where a name can be used for the identification of the ACL instead of memorizing numbers.

For example it is important to avoid the overload of the school network due to unnecessary file swapping and downloads. A simple ACL can deny the FTP access of the students.

Here the whole FTP traffic (ports 20 and 21) is denied in the local network 192.168.1.0/24. Thus the existence of a firewall in case of a school network is an essential requirement from a security point of view. It can contribute to an efficient traffic filtering management and it can ensure the simple separation of the laboratory network from the staff network. Furthermore, the analysis of the network traffic logs created by firewalls can also give clues for the improvement of the applied protection measures.

Computer laboratory usage policy

A computer laboratory usage policy defines when, how and by whom laboratory resources can be used. Its positive effect is that it creates a clear situation by defining possibilities and boundaries. Usual elements of this rule collection are prohibitions of

- interfering with cables and laboratory equipment;
- illegal downloading, file swapping, and copying;
- usage of the equipment for non-scholarly purposes;
- software installation by students;

as well as the regulation of

- availability to students for drop-in use when classes are not in session;
- printing and the related billing;
- how a software installation can be requested by a teacher;
- responsibility disclaimer for lost, damage or theft of personal items left unattended in the labs.

SURVEY ON THE CURRENT PRACTICE

The main aim of our survey was to get a broad picture of the protection level of computer laboratories in secondary schools of Kecskemét. We were wondering which components of the above presented best practice measures are in fact used in everyday practice. The diagrams presented in Figures 4-15 show the results of the evaluation of the questionnaires representing the positive answers with blue and the negative ones by red, respectively. The responses given to the questions related to the physical protection and the protection of the workstations show that about one out of four or less school exploits the cheapest available security options like ACSs and password protection of the BIOS (see Figure 4 and Figure 5).

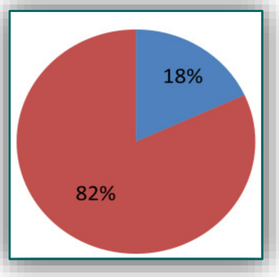


Figure 4. Do you use any kind of lab access control system?

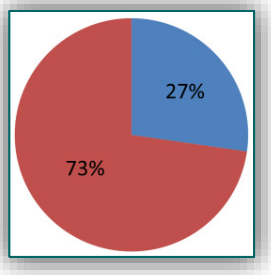


Figure 5. Is the BIOS of the workstations password protected?

However, one can clearly recognize the presence of the security awareness aiming the protection of the operating system and the stored data. The vast majority of schools utilize the built-in security services like authentication mechanisms and automatized partition/folder restore (see Figure 6 and Figure 7).

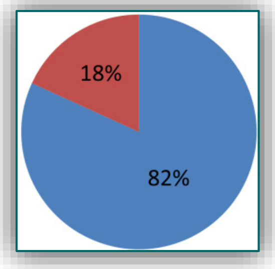


Figure 6. Do the users need login credentials in order to log into the workstations?

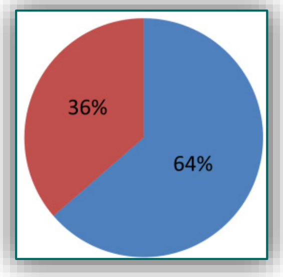


Figure 7. Did you configure a folder or partition based restore solution?

Surprisingly most of the institutions opted for a centralized management despite its significantly higher costs (see Figs. 8 and 9). These systems are mainly based on Microsoft's Windows OS family.

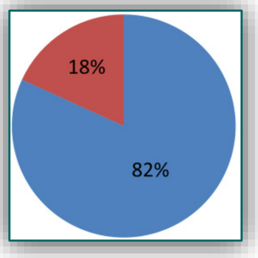


Figure 8. Do the workstations belong to a domain (DC supervised system)?

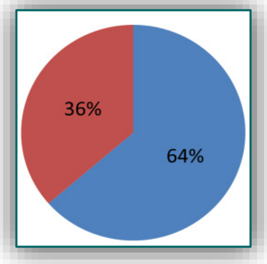


Figure 9. If there is a domain system implemented do you use group policies for workstations and users?

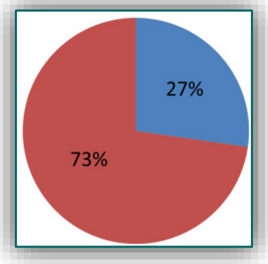


Figure 10. Is denied the access to any external hardware devices (e.g. USB disk)?

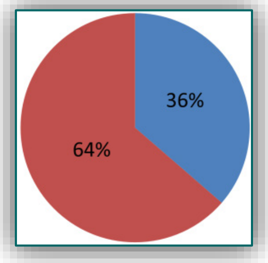


Figure 11. Do you have a backup scheme for the file server?

Although they offer a wide range of security strengthening service only a relatively small amount of them is applied in practice. For example useful and simple-to-configure services like the denial of access to external drives or file server backup schemes do not belong to the applied security measures in most of the cases.

Apparently network protection gets an increased attention, almost three out of four institutions created separate security zones for the laboratory networks and the institutional network. However, 27% of them do not even have a firewall which results in a high risk of cyber-attacks.

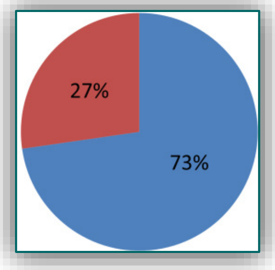


Figure 12. Is the institutional network separated from the network of the labs?

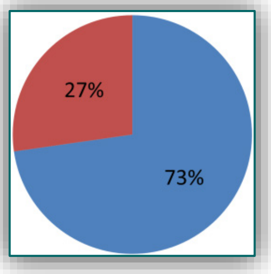


Figure 13. Does your LAN have a firewall?

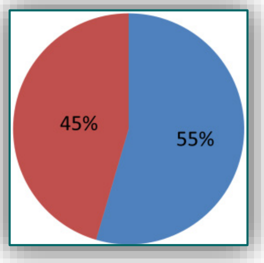


Figure 14. Is there any documentation about your institutional network and IT system?

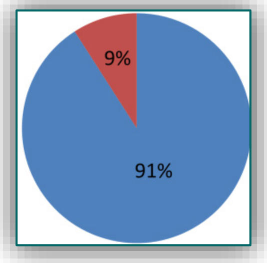


Figure 15. Do you have a usage policy for the computer labs?

More than half of the schools recognized that having a proper documentation of the administered network can significantly simplify the maintenance and troubleshooting activities. Although computer lab rules and policies usually are not very popular between students but almost all of the schools found them to be an indispensable component of the security infrastructure.

CONCLUSIONS

Analyzing the results of the survey one can clearly recognize the existence of security awareness of the institutions in some fields. They strive for the protection of their IT systems but they do not embrace all the available options. Some examples supporting this conclusion are enlisted below.

- Applying group policies but not denying the access to external hardware devices.
- Creating centralized data storage but lacking in systematic backup.
- No emphasis on physical protection of the rooms and workstations despite the promise of the most cost-effective solution.
- Missing computer laboratory or IT system documentation.

Summarizing the experiences we can state that secondary schools should have an increased focus on information security in order to protect the infrastructure and the students as well. There are always reserves whose exploitation could lead to an improved level of security without significant cost increase.

Acknowledgements

We thank system administrators and teachers of secondary schools of Kecskemét for supporting our work by filling out the survey, which made us possible to get a picture about the current regional state of computer laboratory security.

References

[1.] Access control key fobs (2015). https://en.wikipedia.org/wiki/Keychain#Access_control_key_fobs. [Accessed: 9-Jan-2016].

[2.] Ajanovski, V. (2015). Access Control and Monitoring for Campus Computer Labs. Best Practice Document. http://services.geant.net/cbp/Knowledge_Base/Campus_Networking/Documents/CBP-12_access-control-and-monitoring_final.pdf. [Accessed: 9-Jan-2016].

[3.] Backup Types: Full, Incremental, Differential (2015). http://www.enterprisefeatures.com/backup-types-full-incremental-differential/ [Accessed: 10-Jan-2016].

[4.] Bunyitai, Á. (2011). The role of access control systems in asset protection (in Hungarian). A beléptető rendszerek helye és szerepe a vagyonvédelemben, Hardmérnök, Vol. VI. No. 4., pp. 17-25.

[5.] CCNA Discovery 3: Introducing Routing and Switching in the Enterprise (2012), Chapter 8

[6.] Configuring IP Access Lists (2007). http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html. [Accessed: 12-Jan-2016].

[7.] Davis, W., Chi, H. (2011). Cyber threat analysis for university networks via virtual honeypots. ACM Southeast Regional Conference 2011: 354-355

[8.] Deep Freeze (2016) http://www.faronics.com/en-uk/products/deep-freeze/. [Accessed: 10-Jan-2016].

[9.] Gattine, K. (2016). Types of firewalls: An introduction to firewalls http://searchnetworking.techtarget.com/tutorial/Introduction-to-firewalls-Types-of-firewalls. [Accessed: 12-Jan-2016].

[10.] Khosrow-Pour, M. (2014). Encyclopedia of Information Science and Technology, Third Edition, Information Resources Management Association, USA, 2014.

[11.] OpenLDAP (2016). http://www.openldap.org/. [Accessed: 10-Jan-2016].

[12.] Proximity Keyfob (2016). http://www.tdsi.co.uk/proximity_key_fobs.html. [Accessed: 18-Jan-2016]

[13.] Rhodes, B. (2015). Designing Access Control Guide. http://ipvm.com/reports/designing-an-access-control-system. [Accessed: 9-Jan-2016].

[14.] Samba (2016). https://www.samba.org/. [Accessed: 10-Jan-2016].

[15.] Tamper Evident Foil Security Labels Sticker Seals (2016.) http://www.amazon.com/Evident-Security-Sticker-Numbered-Rectangle/dp/B00NGXNFZU . [Accessed: 18-Jan-2016]

[16.] Tamper-evident technology (2016). https://en.wikipedia.org/wiki/Tamper-evident_technology. [Accessed: 9-Jan-2016].

[17.] Thomas, O. (2014). Training Guide: Administering Windows Server 2012 R2, Microsoft Press, Redmond, 2014.

[18.] What is System Restore? (2009). http://windows.microsoft.com/en-us/windows/what-is-system-restore#1TC=windows-7. [Accessed: 10-Jan-2016].

ACTA Technica CORVINIENSIS
BULLETIN OF ENGINEERING

ISSN:2067-3809