American-Eurasian Journal of Scientific Research 10 (1): 41-44, 2015
ISSN 1818-6785
© IDOSI Publications, 2015
DOI: 10.5829/idosi.aejsr.2015.10.1.22125

Construction of the Protection for Students from Cyber Extremism in a Cloud Computing of Educational Services

V.A. Oshurkov, V.N. Makashova, L.S. Tsuprik and E.V. Luk'janova

Nosov Magnitogorsk State Technical University, Magnitogorsk, Russia

Abstract: The relevance of the topic based to the extensive use of modern information technologies in educational and increasing requirements for the content of Internet content. This article describes the mechanisms to counter various threats, including ideology of cyber extremism. The basic mechanisms of information security educational institution (filtering and monitoring) from the point of view of the incoming and outgoing data stream. Recommendations on the use of software products that provide information security for different hardware configurations educational institutions. Considered the questions of students education and the problem is identified shortcomings of the current systems, which manage information security policy of educational institutions. Prevention mechanisms (at the technical level) phenomena cyber extremism are fundamental to the protection of the students and, as a consequence of a good students experience of those services.

Key words: Cyber extremism · Cyber extremism · Information security · Content filtering

INTRODUCTION

Modern Internet technologies become available and have an important place in almost all areas of human activity, including education. «Drawing on the experience of developed foreign countries, an excellent solution for optimizing the learning process are cloud technologies, which are accessed through the Internet» [1]. Most Popular Now the term «cloud computing» began to be used in the world since 2008. In educational institutions of Russia cloud services initially appeared mainly as free hosting of postal services. Numerous other tools of cloud computing for education were not used due to lack of information about them and the lack of practical skills of their use for educational purposes [2]. The best way to prepare students to work with the latest technology-the introduction of these technologies in the educational process [3].

MATERIALS AND METHODS

The analysis we were able to identify two types of cloud services, education [4]:

- Services proprietary educational institutions:
- Personal virtual computer (hereinafter PVC). Single point of access to services, which is formed on the basis of cloud computing technology. Each student created a single personal computer with a virtual personal profile.
- Designer nonlinear schedule. With this module, teachers together in real time can plan forms of those or other activities.

Existing services on cloud technologies:

- Electronic Journal. Is an analogue of a paper magazine, with the ability to lock fields for correction, after a two-week period.
- Virtual lessons, online meetings, video and voice communication.
- Sites classes and groups. Web development classes and groups to share documents and information with the help of a specialized program «SharePoint Online 2010».
- Documents on the Internet. View, edit and share Microsoft Word files on a network using SharePoint and Office Web Apps.
- Project Planner in real time allows you to set goals, monitor progress and track changes over time.

Corresponding Author: V.A. Oshurkov, Nosov Magnitogorsk State Technical University, Magnitogorsk, Russia.

An analysis of educational services on cloud technologies, we can say that the introduction of such a modern innovative approach to learning in higher and secondary school will provide [5]:

- Reduce costs and ensure flexibility. All services run on remote servers and maintained by representatives of cloud technologies, indicating a high productivity and reducing costs.
- Partially protected data. To date, the «cloud» provides two basic principles of information security: data integrity - protection against failures, leading to loss of information; confidentiality and availability of information for all authorized users.
- Effective use of educational areas. There is no need to allocate separate and specially equipped rooms and computer classes.
- Produce a qualitatively new level of contemporary knowledge. Students have the opportunity to be in the process of learning at any time and in any place, in the presence of the Internet [6].
- A more effective interactive learning process.
- The ability to quickly create, adapt and replicate educational services during the training process.
- Centralized administration software and information resources used in the learning process.
- The most effective use of existing computer systems, as to cloud services brought the minimum hardware requirements [7].

Dedicated dignities lead to the following conclusion Educational services in the cloud technologies are enormous prospects of development of the educational process, but there is a possibility of cloud technologies vulnerability to attack of cyber extremists. After all, young people are most susceptible to the destructive influence. Among young people because of their social characteristics and severity of the perception of the environment is the part of society, in which the fastest accumulation and realization of the negative potential for protest. Last year, 132,000 teenagers committed crimes more than 284 thousand minors, police set up a preventive register. The state in 2014 in Russia there is 141 youth group of extremist nature. A number of crimes are growing every year [8].

Trends in the development of the Internet can effectively predict the development opportunities of cyber extremist's organizations developing new forms and methods of information and psychological impact and conducting their approbation, which allows quickly and efficiently distribute cyber extremist's messages. Due to the nature of low level of detection and the lack of experience in defense, in most cases it is impossible to determine at the time of cyber extremist message and students across the tricks of cyber extremists [9].

To successfully address the phenomena of cyber extremism among young people, it is necessary to be clear about the ultimate goal. Primarily, it is necessary to allocate cyber extremism particularly, to prevent further [10]:

- Cyber extremism constantly fueled uncertainty in the position of a young man and his unsteady views on what is happening;
- Cyber extremism manifested in the Company and the Group, which has a low level of self-esteem or conditions contribute to ignore the rights of the individual;
- This phenomenon is characteristic of communities rather than the so-called «low culture» as a culture torn, twisted, is not integrity [11].

In order to ensure information security and as a consequence of restrictions on students cyber extremism phenomenon, we propose to use technological protection measures (software, hardware and hardware and software systems).

RESULTS

The need for technological protection measures dictated by the fact that the Internet-a source of information for which no one is responsible and the probability of getting out of it inaccurate, abusive, pirated or illegal for other reasons information is very high [12].

Consider the basic mechanisms of technical means of protection:

- Protection of external connections

To protect the external connections used cryptographic protocol SSL (Secure Socket Layer). This protocol uses asymmetric public-key cryptosystem. To implement SSL connection requires that the server has an installed digital certificate. Digital certificate - a file that uniquely identifies the user and the server.

SSL provides secure communication by combining two of the following elements:

- Authentication. A digital certificate is tied to a particular domain on the Internet and CA conducts inspections, confirming the authenticity of the organization and only then creates and signs a digital certificate for this organization.
- Encryption. Encryption-the process of converting information into an unreadable for all species, except for a specific recipient. It is based on the need for e-commerce guarantees confidentiality of information transmission and the impossibility of its falsification.

Necessary to identify the springtime compounds in order to protect data against tampering and prevent the following phenomena:

- «Spoofing" (spoofing). Fake sites designed to provide a credit card number.
- The falsification of data. The content of a transaction can be intercepted and maliciously or accidentally altered during transmission.

- Authorization through specialized catalog «Active Directory»

Service «Active Directory» (Active Directory Service) is a distributed database that contains all domain objects [6]. Domain environment «Active Directory» is a single point of authentication and authorization of users and applications across the object.

The advantages of «Active Directory», which will protect the educational institution from cyber extremists attacks [6]:

- A single point of authentication. When using «Active Directory» all user accounts are stored in one database and all computers are turning to it for authorization.
- Single point of policy management. When using a single directory «Active Directory», all users and computers hierarchically distributed by organizational unit, each of which applies uniform group policies.
- Increased level of information security. Using services «Active Directory» significantly increases network security through a single and secure storage accounts and use secure authentication protocol «Kerberos».
- Integration with classes and departments of applications and equipment. «Active Directory» complies with LDAP, which is supported by other systems.

- Monitoring and analysis of network traffic using specialized software.

Monitoring and analysis of network traffic needed in order to more effectively diagnose, predict and solve problems of cyber extremism [3]. Today there are many different tools that allow you to help administrators and general users to monitor and analyze network traffic.

To analyze and monitor the network using special protocols and utilities. However, not all informative in terms of available capacity in their arsenal analysis. Experienced specialists identify the program «WireShark», which has sufficient analytical capabilities and can run on different operating systems [3].

- Control of user actions in the network and content filtering for cyber extremists messages

Monitoring and analyzing user actions allow monitoring the transfer of confidential information outside the organization through various channels and using a variety of applications [8]. However, the primary function of such systems is detailed logging user activity.

There are a number of software products for monitoring and analysis of users, the main functions are: tracking user interaction in a network of educational institutions and what applications, network services, social networks are used; recording and analysis of the contents of communication or correspondences; maintaining tracking user activity by various means of communication, including voice communication; forming a picture of the day of the user; reporting on the activity of users of varying degrees of detail.

DISCUSSION

The result of applying the solution will achieve the following benefits: reduced risk of leakage of confidential information; monitoring and recording user actions, their communications and as a result, detection and suppression cyber extremist’s messages; support and analysis of different data representation formats.

The second problem-this is incompetence of students, teachers to cyber extremism and information security.

«Administrators in schools have a different experience with computers and even a layman should be able to create and maintain a filtering policy. The educational process includes a number of different areas of science and filtering should be comprehensive, customizable and also provide protection against the latest threats» [1].

CONCLUSION

We offer carry out the following organizational measures to improve the competence of teachers to students cyber extremism and information security:

- Presentations, organizing interviews to enhance the knowledge of students and teachers in the field of cyber extremism;
- Suppression of facts spread cyber extremists containing incitement to social, racial, national and religious hatred and extremist literature;
- Implementation of consistent action on the identification and application of statutory measures to persons involved in cyber extremism activities.

Thanks to the use of technical protection mechanisms and organizational measures can not only provide a secure connection for data transmission, supervise the work and activities of students, attendance tracking of Internet resources, but also to identify and prevent the spread of the facts in the cloud educational services of cyber extremism material nature. All this will restrict students from inappropriate content and thus prevent the negative development of students.

REFERENCES

1. Makashova, V.N., 2013. Mechanisms to counter cyber extremism and cyber terrorism in the education system. Fundamental'nye issledovanija, 10(9): 2054-2059.
2. Baranov, A.S., 2011. Youth extremism: Status, Trends and Challenges response. http://www.nbrkomi.com.
3. Greg Sh, 2012. Network Traffic Monitor. http://en.community.dell.com/techcenter/networking/nms/b/weblog/archive/2012/09/21/simplified-network-traffic-sniffing.
4. Grunistaja, O.S., 2013. Cloud technology as a tool for organizing the learning process in the Russian universities. F?N-Nauka, 1(16): 33-34.
5. Oshurkov, V.A. and V.N. Makashova, 2014. Mechanisms to optimize program management of IT-projects. Sbornik nauchnyh trudov SWORLD, 1(11): 66-72.
6. What is SSL, 2013. https://www.globalsign.com/en/ssl-information-center/what-is-ssl.
7. Storozheva, E.V., A.S. Valeev, T.V. Kruzhilina and A.N. Sergeev, 2010. Modeling of the process of formation of economic literacy of students in the structure of additional education university. Magnitogorsk: Magnitogorsk State University, pp: 29.
8. Content filtering, 2013. http://www.microtest.com/it-infrastruktura/informacyonnaya-bezopasnost/1055.
9. Chernova, E.V., 2013. Mechanisms to counter cyber extremism and cyber terrorism in the education system. Fundamental'nye issledovanija, 10(9): 2075-2079.
10. Chris Gee, 2014. Using Social Media and Brand Advocacy to Counter Cyber Extremism. https://www.linkedin.com/pulse/20140530135737-3222728-using-social-media-and-brand-advocacy-to-counter-cyber-extremism.
11. Gordon, S., 2010. Cyberterrorism? Available at: http://www.packetsource.com/article/laws-andregulations/39683/cyberterrorism.
12. Denning, D., 2010. Cyberterrorism. Available at: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.