ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 11 , November 2019

Protection of System from an Unauthorized Leak of Confidential Information

GayratJuraev, ObidjonBozorov,DadakhonSharofov

Associate Professor, National University of Uzbekistan named after MirzoUlugbek, Tashkent, Uzbekistan
PhD student, National University of Uzbekistan named after MirzoUlugbek, Tashkent, Uzbekistan
Leading specialist the department of Development and Support of Automated banking system of OFB, Tashkent, Uzbekistan

ABSTRACT: In this article, the control of confidential information movement of government organization's information systems and their protection against unauthorized access will be discussed. Government agencies have proposed the creation of a national DLP system for predicting and preventing the leakage of personal information in order to effectively ensure and organize the security, usability and protection of confidential information on existing national information resources.

KEY WORDS: confidentiality, DLP (Data Leak Prevention), data leakage channel, FTP control, Email control, Skype software control, IM control, HTTP control, Cloud control, DLP gateway, Print control, Key Logger, File control, «Electronic Government».

I. INTRODUCTION

The secrets of state organizations or other data which consisting of state secrets protected by law, as well as personal data are required to take necessary program and organizational and technical measures to protect confidential information and prevent their unauthorized access by Legislation of the Republic of Uzbekistan. Taking into the consideration of these factors, predicting and eliminating unauthorized leakage of confidential information in government agencies can be considered one of the most actual problems of today.

Nowadays, our government is paying greatly attention to the problems of information security. For example, developed and improved laws and regulations in the field of information security are a good example of this.

The information used in the corporate information system of any modern organization is an important material asset to ensure its sustainability, growth and competitiveness. This includes information about government secrets, intellectual property, customer information, financial performance and business secrets of the company, customer and employee personal information, technological «know how », competitive analysis and many other types of knowledge. Leakage of confidential information from the corporate environment and its users is also a risk for business.

Properly organizing information security policy and implementing it is the basis for successful development for any modern organization, including government agencies. Compliance with the international and interstate standards in the field of information protection is essential for the sustainable operation of government organizations. To ensure the security of data, each organization should develop and maintain databases, the processes of information technology management, and provide the integrity, usability and confidentiality of information.

II. LITERATURE SURVEY

DLP is considered as a paradigm shift in information security, it addresses risks; these risks are focused around handling certain solution to discover, monitor and protect confidential or sensitive data wherever it is stored or used, across endpoint, types of data with information security risk, such as personally network, and storage systems[1]. For this the effective solutions are available. This paper presents best practices for preventing leaks, enforcing compliance, protecting company’s brand value and reputation in organization.DLP solutions help to protect data from going outside company [5].

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 11 , November 2019

III. MAIN PART

Confidentiality: The status of the information and its media, preventing unauthorized access or unauthorized documentation.

Leakage of confidential information is uncontrolled dissemination of confidential information from the organization or a particular person.

Data leakage channel is called an outflow channel and refers to the physical path from the source of confused information to the malicious person who receives confidential information. This way the information can be leaked or unauthorized access to stored information. In order for the data channel to appear, the malicious person must have the means to receive and record appropriate information.

In the security of information systems, more attention is paid to external threats such as spam and "denial of service" such as fishing attacks, viruses and advertising programs. In fact, internal threats to the information system can do far more serious harm than external threats. IDS, IPS, DLP, SIEM, NBAD systems are currently used in the fight against internal threats.

Explanation works should be taken to safeguard the confidentiality of the information which entrusted to employees, as the leakage of confidential information is often caused by employees' ignorance or misunderstanding of the importance of compliance with the rules. In an international practice, DLP (Data Leakage Prevention) systems are proposed as an effective way to prevent such incidents.

DLP (Data Leakage Prevention) is a state-of-the-art technology for protecting confidential information in the information system from unauthorized access using software or hardware. Leakage channels can be network (for example, e-mail) or local (using external data collectors).

The DLP system tasks are followings [1]:

- monitoring the life cycle of the confidential information that stored on the servers, workstations and databases;
- analyzing of data from the protected information systems or the flows of data from networks;
- controlling of actions copying of confidential information to the external media, printing and storage the confidential information;
- investigate regularly incidents of confidentiality data and identify intruders;
- Monitoring the work time of employees;
- properly forming the politics of information security in the organizations, implementing it and defining the illegal actions of employees;
- creating of statistical and reporting documents in terms of moving confidential information.

The proposed protection system consists of the following parts:

- Controlling and monitoring center (server part);
- DLP gateway located between server-side and network gateway;
- Client parts of the system installed on the computers of all users (Figure 1).

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 11 , November 2019

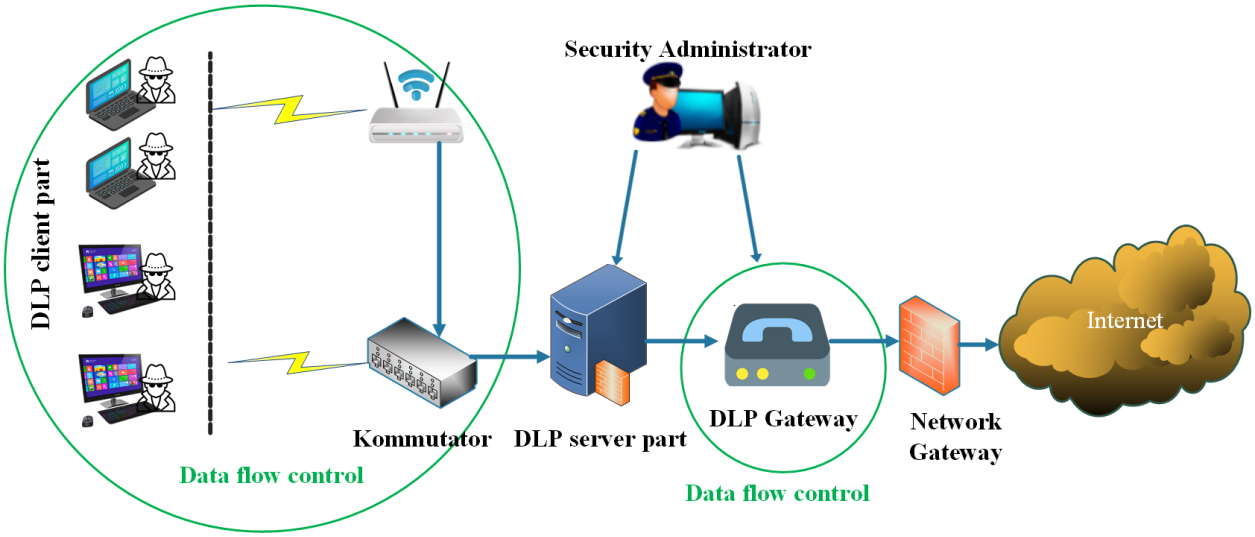

Figure 1. The general structure of the DLP system.

To define the unauthorized leakage of confidential information, protection system controls external flow. In all users of the organization installed on client's part, processing and storage of confidential information will be managed.

The modules of Data Leakage Prevention (DLP) system

The proposed confidential information protection system consists of several modules, each of those controls specific data transmission channels and they are follows:

- Email control module. This controls all emails (Gmail, umail.uz, Mail.ru, etc.);
- IM control. This controls social networks and messengers;
- FTP control. This controls the information transmitted through FTP protocol;
- HTTP control. This controls the exchange of files and messages through HTTP / HTTPS protocols;
- LDAP synchronization manager. This monitors data that sent to cloud storage;
- Monitoring control. This controls the data displayed on the computer's monitor and web-camera;
- Print control. This controls the meaning of the documents submitted for printing;
- Device control. This controls the data that is being written to external information medium;
- Key Logger control.This controls the information input from the keyboard and the data copied by the keys;
- Archive and file control. This manages operations under files containing confidential information in server and network folders;
- Skype application control. This controls the conversations, calls, SMS and file's flows via Skype.

Analysis of all information in the computer system significantly reduces the speed of the computer system. Protective systems should firstly be able to distinguish sensitive information from all incoming data. Then, they have to control over the life cycle of classified information. In order to extract confidential information, linguistic analysis, statistical analysis, search by regular expression, comparison of control summaries, and search by key are used.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 11 , November 2019

The use of DLP systems in government agencies enables you to:

- identifying and categorizing data that are critical to protecting data using a variety of data analysis mechanisms;
- use multiple approaches to categorizing data;
- content analysis (linguistic technologies, including vocabulary analysis and stemming (counting grammatical word forms), regular expressions, digital footprints);
- analysis of official signs (document grip, embedded symbols, document type and scope), control of large enterprise information flows, monitoring data channels, compliance with applicable security standards for important data movement;
- scanning stored files to determine the location of important data, tracking user behavior, writing and analyzing their communications [2].

IV. CONCLUSION AND FUTURE WORK

Nowadays, license prices, including the right to purchase and use DLP systems, which are typically used for 12 months, are as follows(prices are indicated for 250 users):

- DeviceLock DLP - $ 23,000;
- Symantec Data Loss Prevention (DLP) Suite - $ 20,000;
- McAfee Total Protection for DLP - $ 22500.

These figures show that the importation of the DLP system alone will result in millions of dollars a year from the national budget. In the view of the above, the development of a national DLP system that integrates with the system of government agencies remains one of the most important issues of modern information security. Creation and implementation of the national DLP system will ensure reliable protection of national information resources. At the same time, the issue of ensuring reliable protection of information resources in our country requires the use of national and foreign means of information security certified by the authorized body on information security.

REFERENCES

[1] Radwan R. Tahboub, Yousef Saleh. Data Leakage/Loss Prevention Systems (DLP) NNGT Journal: International Journal of Information Systems. Volume 1, 2014. –P. 13-19.
[2] Juraev G., Bozorov O. Problems and solutions to protect confidential information in the Republic of Uzbekistan in the "Electronic Government" // Tashkent, April 12, 2019. 108-111 p.
[3] On additional measures to ensure computer security of national information and communication systems. Decree of the President of the Republic of Uzbekistan -T., September 5, 2005, No. PQ-167.
[4]On the protection of information in the automated banking system. Law of the Republic of Uzbekistan. -T., April 4, 2006, ZRU-30
[5]Preeti Raman, HilmiGüneşKayacık, and Anil Somayaji,"Understanding Data Leak Prevention",ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA) Journal, JUNE 7- 8,2011.