IMPLEMENTATION OF SECURITY SYSTEMS FOR PREVENTION OF LOSS OF INFORMATION AT ORGANIZATIONS OF HIGHER EDUCATION

The 12th International Conference on Information Technology: New Generations (ITNG 2015), April 13-15, 2015, Las Vegas, Nevada, USA

Askar Boranbayev
Nazarbayev University
53 Kabanbay Batyr Ave,
010000 Astana, Kazakhstan
aboranbayev@nu.edu.kz

Mikhail Mazhitov
Nazarbayev University
53 Kabanbay Batyr Ave,
010000 Astana, Kazakhstan

Zhanat Kakhanov
Nazarbayev University
53 Kabanbay Batyr Ave,
010000 Astana, Kazakhstan

***Abstract*— In this paper we discuss our experience of implementation of Data Loss Prevention (DLP) system at our University. The DLP system helps to analyze, control, monitor, block and protect data at the University. With the help of the DLP system and encryption we are able to protect and control the confidential data about our clients, HR data, intellectual ownership data, legal and financial documentation, official letter exchanges with partners and clients, academic and research data, etc...**

Keywords — information security; data loss prevention; software; information system; data.

I. INTRODUCTION

Before the decision about implementing the DLP system at our University was made, it was actively discussed whether it will be useful for the University and whether it would be worth the money spent. Universities are usually open organizations of education and have open-doors policy, where people should feel free to work, receive education, conduct research, and exchange knowledge without being intimidated by anything. However, the University and its affiliated organizations, have a sufficient amount of official, confidential and restricted data, which must be protected. Loss or dissemination of confidential information could result in property damage, financial loss, loss of reputation of the University, insolvency or eventually lead to the unprofitability.

Up until recent times the dissemination of information could be controlled by the existing institutional and administrative means, technological means using group policies, allowing access only to a limited number of persons. Now, during the growing market in information technology, we need to worry about the leakage of confidential information, because attackers similarly seek to use the latest tools in the field of information technologies and methods to achieve their selfish goals.

In accordance with The Law of Republic of Kazakhstan "On Personal Data and Its Protection", aimed at ensuring privacy and protection of personal and family secrets, and increased state regulation in this area, for non-compliance by the owner, the operator or a third party of measures to protect personal data (the Law of the Republic of Kazakhstan dated May 21, 2013 № 95-V «On amendments and additions to some legislative acts of the Republic of Kazakhstan on issues of personal data and protection") - sanctions will be applied on entrepreneurs, organizations and all the legal entities or physical entities. With substantial harm to the rights and legitimate interests of individuals for this is provided and criminal liability.

In order to ensure the necessary level of information security of the University it was decided to implement a system of Data Loss Prevention (DLP). DLP system helps to analyze, monitor, track, lock and protect our data. Jointly using encryption and system DLP, we can protect a wide range of information: customer data, intellectual property, legal and financial records, correspondence with customers and partners, and so on. The University has acquired McAfee DLP system, which has the necessary technical and functional capabilities, broad development prospects and excellent integration with various McAfee solutions under a single toolkit. We would like to note that McAfee solutions today are widely used in a number of major institutions in Kazakhstan.

Let's look at the DLP and reveal the theme. How it is going to be used at the University? Which directions were chosen and what specific modules were implemented?

II. ABOUT THE SYSTEM

There are certain areas that we think are particularly in need of protection. These areas include:

978-1-4799-8828-0/15 $31.00 © 2015 IEEE
DOI 10.1109/ITNG.2015.147

– Financial & economic (procurement documentation, financial information, etc…);
– Legal (internal documentation, contracts, confidential information about employees, even after termination of their employment relationships, etc…);
– Human Resources (data on staff and students, personal data, reports, etc…);
– Educational and research (tests, examinations, research and development information, intellectual development, information about students, research projects, etc…);
– IT (databases, their structure, IT management information, logins and passwords, copyright developments in IT, etc…);

It is known that for protecting and controlling the sensitive and confidential information it is necessary to implement organizational and technological measures to protect the information. In this article, we are not describing how organizational measures were implemented and organized. Let's deliberately accept that all of the organizational measures have been implemented in terms of the University and are already working properly. Also, let's accept that the University's legal framework meets the necessary requirements and all the necessary internal rules and regulations are already in place.

With McAfee DLP system we are able to provide:
– protection of information assets and critical information to the University;
– monitoring in Online mode to protect information;
– protection from leakage of confidential information through the official web e-mail;
– control over opening or closing of PC ports (USB port, CD-DWD drives, ports for reading CardReader, …) and their monitoring;
– control over connection of various equipment to the PC;
– transparency of workflow for the upper management and security services;
– structuring and systematization of data;
– detection and protection against spam mailings.

Additional services that may be provided through DLP:
– protection against malicious software;
– the formation of detailed reports that demonstrate to auditors and other interested parties full compliance with internal and regulatory requirements, as well as for administrative decision-making;
– saving the usage of Internet traffic;
– optimization of the corporate network;
– improve the efficiency of the work of the staff.

The McAfee DLP system, that was established at our University consists of the following modules:
1) DLP Discover - subsystem provides a classification and indexing of data;
2) DLP Prevent - subsystem, resources aimed at blocking the transmitted information;
3) DLP Monitor - subsystem that provides continuous monitoring of all data storage and indexing of the resulting analysis of information;
4) DLP Manager - subsystem control and optimization of security policies provides a complete security management system;
5) DLP Endpoint - subsystem that protects data on endpoints, including the client software (agent) and server software;
6) ePolicy Orchestrator (ePO) - a centralized management console that allows you to centrally configure and manage data protection policies, deploy and update software agents, monitor real-time events, and generate reports to ensure regulatory compliance.

The system also has additional devices in it:
a) Web Gateway - a subsystem that provides control over information transmitted via the Internet and protection against web threats.
b) Endpoint Encryption for Files and Folders - encryption module for data.
For more information about these modules and subsystems can be viewed on the official website of the manufacturer. (http://www.mcafee.com)

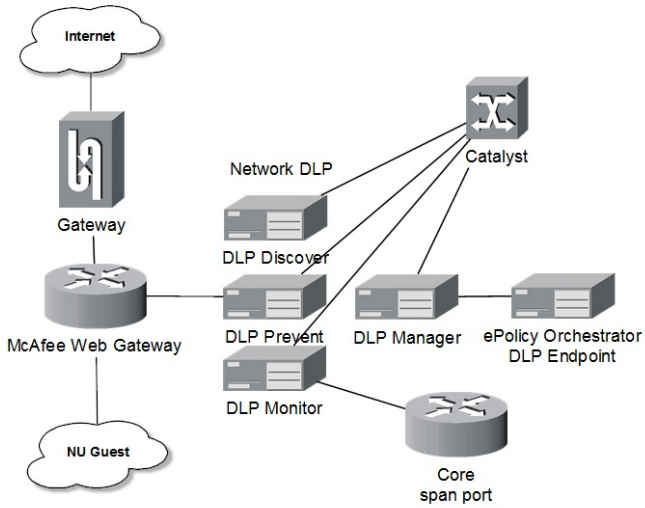


Diagram 1: Logic diagram showing how modules are interconnected in the implemented DLP system at the University.

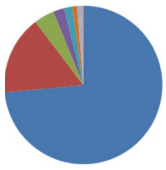
When implementing a DLP system, we developed the architecture of the system, as reflected in Fig. 1. Then we carried out on the implementation, installation, configuration, testing of the system. The necessary customization and optimization of the information system was performed. [5],[6]. The server equipment and software have been set up in the main Data Center of the University.[4] We performed custom installation of agents on the areas that have been mentioned above and on office computers, entering the risky area of possible leaks.
We have set up all the appropriate rules and policies of DLP - in accordance with the directions that have been identified by internal regulations and documentation of the University:

- *Policies = 11*
- *Rules & Regulations = 49*
- *Incidents found = 662*

According to the results of set policies and regulations in the amount specified above for a certain period we have recorded 662 cases of transmission of potentially sensitive information.

During testing, it was found that in some cases the policy and rules established for the protection of web e-mail is not always correctly triggered. It was found that the filtration (the set up rule) of web e-mail worked only if the user is using the browser Internet Explorer, and does not work when using the browser Google Chrome, Mozzila, Firefox or Safari. This problem was solved by installing additional subsystem called Web Gateway, since the University is not using protocol icap, with which the DLP Prevent fulfills its function. Other than the protection of web e-mail - the Web Gateway subsystem also solves many other tasks, such as prevention of transmission of data based on keywords, prevention of transmission of credit card data.

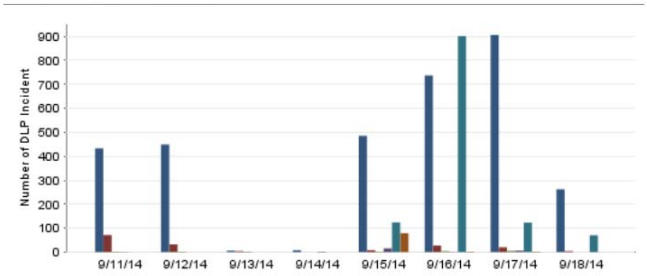
Table 2



Category name	Hits	
Parked Domain	70 929	73%
Spam URLs	15 591	16%
Anonymizers	4 048	4%
P2P/File Sharing	2 164	2%
Malicious Downloads	1 597	2%
Anonymizing Utilities	990	1%
Spyware/Adware/Keyloggers	700	1%
Phishing	481	0%
Potential Hacking/Computer Crime	18	0%
Browser Exploits	2	0%

From Table 2 we can see the distribution of Internet requests by category of security, resulting subsystem McAfee Web Gateway. Having this statistic can make the necessary adjustment to policies and rules for a necessary category. We are able to generate various kinds of reports and graphs with a time interval, thanks to the useful functionality and built-in tools.

DLP Endpoint allows us to provide security on users' computers. We can install a McAfee agent on user workstations, through which we can install DLP Endpoint and other McAfee solutions. Thus, all the host-management products are united in a single interface. To the user it looks like one icon on the control panel, but actually DLP Endpoint runs several processes in the system, thereby using up a lot of resources of your PC. Nevertheless, one can argue that the DLP agent is resource-intensive software, as its resource consumption depends on the number of tasks that are put in front of him by the administrator of the system. Simply put, the higher the security policies specified in the management console, the more resources will be used by the end-point agent. Also, it is worth noting that we can adjust the agents so that they will yield to other processes running on the operating system of the endpoint, but the work of the agent in the low priority affect the quality of mining of security rules.



Time->Policy	Number of DLP Incident
September 11, 2014	507
Investigation {admin}	433
spam {admin}	71
Students {admin}	2
keylogger user {admin}	1
September 12, 2014	483
Investigation {admin}	449
spam {admin}	32
Students {admin}	2
September 13, 2014	12
Investigation {admin}	6
spam {admin}	4
Students {admin}	2
September 14, 2014	10
Investigation {admin}	8
keylogger user {admin}	2
September 15, 2014	713
Investigation {admin}	485
Printers {admin}	124
Simultaneous_Interpretation_System {admin}	79
keylogger user {admin}	15
spam {admin}	8
Students {admin}	2
September 16, 2014	1672
Printers {admin}	901
Investigation {admin}	737

In conclusion, it should be noted that the correct setting and applying of the DLP system can fully perform the functions of protection against loss and unauthorized use of information. This system needs to be customized and set up based on the business rules of the organization.

REFERENCES

[1] Law of the Republic of Kazakhstan on Personal Data and Its Protection.

[2] Information Security Concept of the Republic of Kazakhstan till 2016. Source: Information System "Paragraph"

[3] State Standard of the Republic of Kazakhstan "СТ РК ИСО/МЭК 27001-2008". Information technology. Methods and tools to ensure the safety of information security management system. Requirements. Source: Inforamtion System "Paragraph".

[4] Boranbayev, A.S., Belov, S., Data Center Design and Implementation at the University. Proceedings of the 2012 *International Conference on Computer Design* (CDES), USA, Las Vegas, Nevada, July 16-19, 2012, p.124-126.

[5] Boranbayev, A.S., Boranbayev S.N., Development and Optimization of Information Systems for Health Insurance Billing. IEEE The 7th International Conference on Information Technology: New Generations (ITNG 2010), Las Vegas, Nevada, USA, April 12-14, 2010, p.1282-1284.

[6] Boranbayev, A.S. Defining methodologies for developing J2EE web-based information systems, Journal of Nonlinear Analysis: Theory, Methods & Applications, Volume 71, Issue 12, 15 December 2009, USA, p. e1633-e1637. ISSN: 0362-546X.