MedCrave
Step into the World of Research

International Robotics & Automation Journal

The Process and Methods of Implementation of Data Loss Prevention Systems in the University

Abstract

With the computerization of business activities in higher education institutions and issues with keeping the data secure information security vendors quickly perceived a new market opportunity. In this article we discuss our experience of implementation of Data Loss Prevention (DLP) system at our University. The DLP system helps us 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

Review Article

Volume 4 Issue 1 - 2018

Askar Boranbayev[1]*, Darkhan Kanafin[2] and Mikhail Mazhitov[2]

[1]*Department of Computer Science, School of Science and Technologies, Nazarbayev University, Kazakhstan*

[2]*Nazarbayev University Library and IT Services, Nazarbayev University, Kazakhstan*

***Corresponding author:** Askar Boranbayev, Department of Computer Science, School of Science and Technologies, Nazarbayev University, Kazakhstan, Tel: +77011562459; Email: aboranbayev@nu.edu.kz

Received: November 05, 2017 | **Published:** January 03, 2018

Overview

Disclosing the topic of using the Data Loss Prevention (DLP) system in the Autonomous Educational Organization "Nazarbayev University" (University), it should be noted that the question of the appropriateness of using the system in the process was discussed quite actively. The University is an open organization and for obtaining international education, the information that is provided in the system of the educational process at the University is completely open to all, i.e. there is a formal rule of "open doors". At the same time, the University and its subsidiaries have accumulated a sufficient amount of official, confidential information and information of limited distribution in their activities. The loss or dissemination of such information can lead to material damage, financial losses, loss of the University's reputation, insolvency or, as a result, unprofitable use or commercialization of the business process, mechanism, and services [1-5].

Previously, the dissemination of information could be effectively controlled by available organizational and administrative means, technological means through group policies, providing access to certain information resources only for a limited number of individuals. Currently, to control access to information and especially its transfer by the listed means is not enough, in view of the rapidly developing market in the field of information technologies. Therefore, the problem associated with the leakage of confidential information will be relevant all the time, because attackers similarly seek to use the latest tools in the field of information technology and methods to achieve their own selfish goals. In accordance with the law of the Republic of Kazakhstan "On Personal Data and their Protection" (a reference to this law), violations of this Law, related to unauthorized disclosure of personal data, provide for sanctions in the form of a fine for individuals, officials, individual entrepreneurs, legal entities [6-10]. In case of causing significant harm to the rights and legitimate interests of persons for this, criminal liability is provided.

The peculiarities of information security in educational institutions are the following:

a. Different groups of users. In the university network there can be different categories of users with different requirements for information security: students, teachers, administration, and guests of the university, other staff and freelancers, counterparties.

b. Different ways of access. Since access to some information is carried out through the Internet, the perimeter of the traditional protection zone is constantly changing, often creating the inability to control the transmission of data. Users use their personal devices: laptops, tablets, smart phones, thereby creating certain risks.

In order to ensure the necessary level of information security, the University decided to implement the Data Loss Prevention (DLP) system. The DLP system helps you analyze, monitor, track, block and protect data based on reliable information. Together using encryption facilities and the DLP system, it is possible to protect a wide range of information: customer data, intellectual property, legal and financial documentation, correspondence with partners and customers, etc. The University has acquired the McAfee DLP system, which has the necessary technical and functional capabilities, broad prospects for development and excellent integration of various McAfee solutions under a single instrument. We would like to note that McAfee solutions are currently used in a number of large institutions of Kazakhstan. Let's return to the DLP and explain the topic, how it is used at the University, what areas were chosen to provide protection,

which modules of this solution are involved in the complex, and so on. There are areas that we think are particularly in need of protection.

These areas include:

a. Financial direction (documentation on purchases, agreements, bank information on employees and trainees, etc.);

b. Economic direction;

c. Legal direction (internal documents, contracts of the University and its organizations that impose obligations on non-disclosure of confidential information on each party (legal entity), as well as on all persons who are staff members, including after termination of employment relations with them);

d. Personnel direction (information about employees and trainees, personal data, reports, plans, results of processing personal data);

e. Educational and research areas (tests, exam tickets, scientific developments, intellectual development, research documentation, information about students, research projects)

f. IT direction (databases, their structure, instructions for managing, changing, etc., logins and passwords, authoring developments in the field of IT)

It is known that for the protection and delineation of access to confidential information, it is necessary to introduce organizational and technological measures to protect information. In this article, we do not consider the use of organizational measures and deliberately accept that they are implemented in the conditions of the University and work accordingly. We also accept that at the University the legal framework meets the necessary requirements and there is the necessary internal documentation.

By implementing the McAfee DLP system, we were able to organize:

a. Protection of information assets and important information for the University;

b. Monitoring in the Online mode for information protection;

c. Protection against leakage of confidential information through the service web mail;

d. Control of the opening of the ports of the PC (USB ports, CD-DWD drives, ports for reading Card Reader,) their monitoring;

e. Control of the connection of various equipment to the PC;

f. Transparency of work processes for management and security services;

g. Structuring and systematization of data;

h. Detection and protection from spam mailings.

Additional services that can be provided:

a. Protection against malicious software;

b. Formation of detailed reports demonstrating to auditors and other interested parties full compliance with internal and regulatory requirements, as well as for making administrative decisions;

c. Saving Internet traffic;

d. Optimization of the corporate network;

e. Increasing the efficiency of staff.

The University uses the solution of McAfee, now a division of Intel Security. This solution is presented in two ways: Network DLP and Host DLP. Network DLP consists of four modules, each of which has its own functionality - it's Manager, Monitor, Discover and Prevent. Host DLP from McAfee is referred to as DLP Endpoint. In our organization, both directions are presented, known together as McAfee Total Protection for Data Loss Prevention. All DLP components, like many other McAfee products, are managed using a single console called ePolicy Orchestrator or ePo. Each new product added to the management console is displayed as a separate block in the menu. All policies and rules are set here. The peculiarity of DLA solution from McAfee is that the policies created for the solution of a specific task and for a specific module of the system can be applied to its other modules. That is, if we create a policy for monitoring and analyzing network traffic, the same policy can be used when scanning hosts for such information. Policy management and their integration between DLPs is a task that DLP Manager performs. In addition, it combines some of the system settings of each component and allows you to integrate with the ePo management console.

The McAfee DLP system installed at the University consists of the following components:

a. DLP Prevent - a subsystem aimed at blocking transmitted information. The work of this module is based on the analysis of traffic transmitted over the ICAP protocol, being integrated with the proxy.

b. DLP Discover is a subsystem that provides data classification and indexing, which allows you to detect data at endpoints.

c. DLP Monitor - a subsystem that provides continuous monitoring of all transmitted data, storage and indexing of information received for analysis;

d. DLP Manager - a subsystem for monitoring and optimizing security policies that provides full control over the security policies of the system;

e. DLP Endpoint is a subsystem that protects information at endpoints, including client software (agent) and server software;

f. EPolicy Orchestrator (ePO) is a centralized management console that allows you to centrally create and manage data protection policies, deploy and update agent programs, monitor events in real time, and generate reports to ensure regulatory compliance.

Additional devices:

a. Web Gateway - a subsystem that provides control over information transmitted via the Internet and protection from web threats.

b. Endpoint Encryption for Files and Folders is a data encryption module.

More detailed information about these modules and subsystems can be viewed on the official website of the manufacturer. (Http://www.mcafee.com)

When implementing the DLP system, the system architecture, reflected in Figure 1. After that, work was carried out to install, configure, test the appropriate server and software, selectively install agents in the directions that were mentioned above and on the service computers that fall into the risk zone of possible information leakage. By default, Network DLP offers the administrator of the system a set of ready-made policies for protecting corporate, personal and banking information. All the necessary concepts and templates created in different areas such as corporate confidential, corporate finance, healthcare, human resources, network security, payment card industry and others have already been created by McAfee specialists. These templates can be changed or used in the system created by the system administrator, security policies. When configuring DLP policies, the administrator must take into account many of the nuances. For example, the criteria for sampling an event. It is necessary to take into account the possible ways of transmitting this or that information, the sensitivity of the system to the sampling criteria. Correctly created security policies - a guarantee of rational use of server hardware resources. Obviously, the initial setting of the rules may not bring the desired result, so after some time; the settings are optimized, so that to reduce the number of false positives at which the rule worked, but the information obtained is not of interest. (False positive). Now let's look at the created policies and rules. Most Internet users at the University actively use their personal mobile devices (laptops, tablets, smart phones) and, accordingly, can be infected with malicious programs that, when connected to the University network, begin their active activity. Such malicious programs include spam bots. To identify this kind of viral activity, one of the security policies in the DLP system was created, which will be described in detail. It is known that spam bots mainly use mail protocols, such as SMTP, IMAP. A rule has been created that tracks the transfer of messages across all mail protocols.

Example Rules

In order to exclude the tracking of corporate mail transmission, an exclusion rule was created, the criterion of which was the domain name of the University and, accordingly, one of the part of the name of the e-mail, both the recipient and the sender. Thus, the rule tracked unencrypted traffic (the network DLP is not able to analyze encrypted traffic, the host DLP manages it), by mail protocols, moreover, corporate mail is added to the exclusion of verification and control. As a result, for the 4th quarter of 2016, 10 hosts were found infected with spam bots, whose activities were blocked. Information about the activity of the spam Bot is graphically displayed. The peaks in the graph indicate a large amount of mail sent. (Figure 2), Also, with the help of this rule, vulnerability was eliminated in one of the University sites. On this site was posted a user registration page, not containing the so-called "protection against robots". Thus, all possible bots attacked the server with a large number of registration procedures, thereby causing a rapid filling of databases. For the system administrator, it looked like a huge number of e-mails sent by the site server, with confirmation of the registration procedure. In addition to identifying spam, such a rule was able to identify the use of spyware, key logger. The principle of the key logger's work was that he collected the data entered from the victim's keyboard and transmitted with a certain periodicity using the SMTP protocol. The administrator of the system caused suspicion of regular transmission of e-mail, although the same mailing address was recorded in the fields of the sender and the recipient (Figure 3).

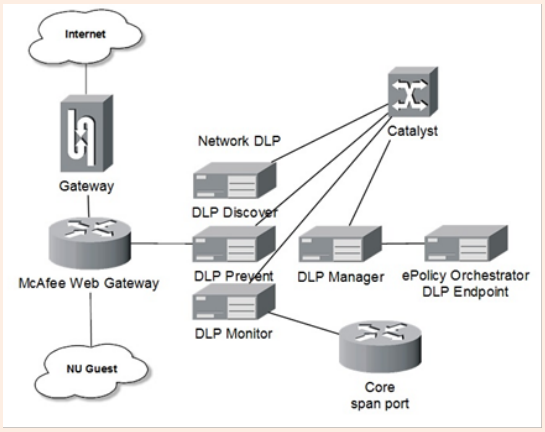

Figure 1: Logical scheme for connecting DLP modules at the University.

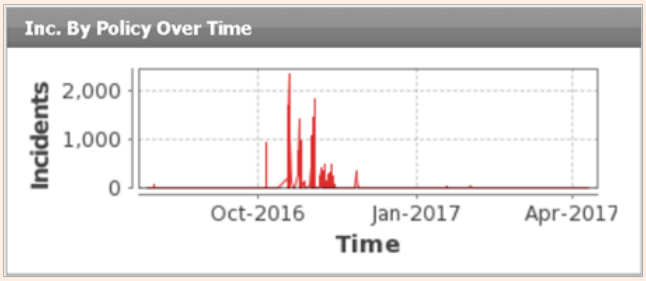

Figure 2: The number of incidents detected in the chart.

Thus, using only one policy, it was possible to investigate 3 types of incidents that satisfied the conditions of one rule. Similar rules can be created arbitrarily much, and their variability allows to really protecting many channels of possible information leakage. The popularity of social networks plays an important role in the procedure for investigating incidents and in identifying intruders. Often among the traffic caught by filters, information is found about the violator's visit to his page in the social network. And given the fact that most of the University's users are students, the procedure for identifying a user is greatly facilitated.

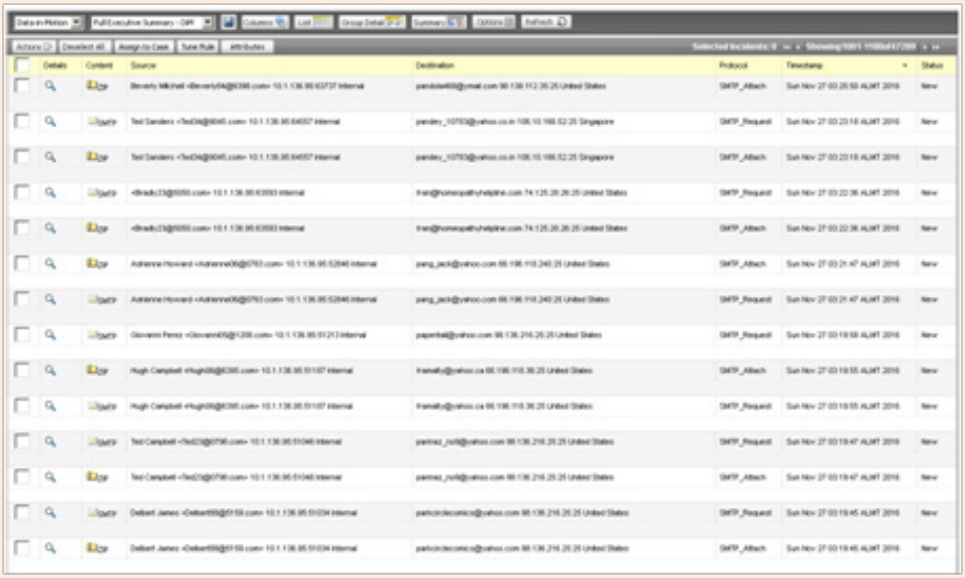

Figure 3: Displays the undesired e-mail in the management console.

Expanding the subsystem DLP Endpoint, it is necessary to say that it, as one of the subsystems of the complete solution of the DLP system, provides security on the users' computers. The main agent McAfee is installed on the user workstations, through which both DLP Endpoint and other McAfee solutions can be installed. Thus, the vendor has integrated the management of all host products into a single interface. For the user it looks like one icon on the control panel, but in fact DLP Endpoint starts several processes in the system, thereby using considerable PC resources. However, it cannot be said that the DLP agent is resource-intensive software, because its resource-consuming capacity depends on the number of tasks that the DLP system administrator will put before it. Simply put, the more security policies are set in the management console, the more endpoint resources will be used by the agent. It is also worth noting that it is possible to configure agents in such a way that they will be inferior to other processes running on the operating system of the endpoint, but the agent's work in a low priority will affect the quality of the security rules [11-13].

DLP Endpoint and Network DLP management environments vary significantly, as does the operation of this subsystem. The main functions of DLP Endpoint are presented in the form of customizable rules, broken down into categories: tagging rules, classification rules, protection rules, discovery rules. There is also a set of rules for device rules, but about them later. Let's take a closer look at the category of protection rules, because it is with the help of these rules that data transfer control is performed. Immediately note that all the rules, which will be discussed later, can be configured for a specific endpoint, an endpoint group, a user or a group of users. So, the protection rules in the version of DLP Endpoint 9.3 used are represented by eleven rules: Application File Access Protection Rule, Clipboard Protection Rule, Cloud Protection Rule, Email Protection Rule, File System Protection Rule, PDF / Image Writers Protection Rule, Printing Protection Rule, Removable Storage Protection Rule, Screen Capture Protection Rule, Web Post Protection Rule. Each of the rules is configured using the wizard. This can cause some inconvenience if you have already created many rules and there is a need to edit several at once. As for functionality, McAfee cannot boast of absolute flexibility of DLP Endpoint custom rules, there are limitations. However, those functions that are presented should be enough to solve most of the tasks that are put before the host DLP. Consider an example of using DLP Enpoint. Task: block transmission of any data from the endpoint. Let's say that we have a computer that only a limited number of people can access, and the information contained on this host is of great importance and confidential status. To solve this problem, it is necessary to create more than one rule, since in addition to transfer to the Internet, it is necessary to prohibit the use of removable media and the ability to print data using peripheral devices. With regard to the last two data channels, you can use Device Rule and disable the connection of third-party devices, but for clarity, exclude this option and perform the task using Protection Rules. Therefore, you need to configure 3 rules: Network Communication Protection Rule, Removable Storage Protection Rule, and Printing Protection Rule. These three should be enough. We will describe in detail the rule by which Internet transmission is carried out.

Network Communication Protection Rule

Wizard offers 7 steps to configure this rule:

a. Which network addresses would you like to protect/exclude? Since the task is blocking the transfer of data to the Internet, this step specifies the entire address pool.

b. Which network ports would you like to protect / exclude? To block the Internet connection, we specify ports 80,443.

c. The third step is to choose which type of traffic you want to track incoming or outgoing, specify outgoing traffic.

d. It is suggested to select the category of applications for

blocking the transfer of data. By default, the rule applies to all applications.

e. In the fifth step, you need to select the tag assigned to the transferred files by the tagging rules, but since we need to block the transmission of any data, there is no need to specify a tag.

f. In the sixth step, you must select the actions that will be taken when an incident is detected. You can specify checkboxes in the boxes: block, track and notify the user.

g. At the last step, you are asked to select the users to which this rule will apply.

Such simple manipulations blocked the transfer of any data to the Internet. The detected events are quite informative and contain the addresses source, destination, evidence, detection time and much more. Unfortunately, there are no informative dashboards similar to those in the network DLP, but all the necessary information can be obtained from reports generated in ePolicy Orchestrator.

Conclusion

We would like to say that systems like DLPs are not a panacea for insider trading. An attacker, if desired, can always steal information, by whatever means. There are many ways to bypass protection. But it is worth noting that, in addition to the basic functionality of the security system, such DLPs provide increased user loyalty. With the correct submission of information on the implementation of the system, the insider thinks about the risk of being exposed and, possibly, will not take measures to steal data, because its actions can be tracked.

Acknowledgement

My research project was fully sponsored by Nazarbayev University.

Conflict of Interest

No conflict of interest.

References

1. The Law of the Republic of Kazakhstan on Personal Data and their Protection. Source: IP Paragraph.
2. The concept of information security of the Republic of Kazakhstan until 2016. Source: IP Paragraph.
3. ST RK ISO / IEC 27001-2008. The state standard of the Republic of Kazakhstan. Information technology. Methods and means of ensuring the security of the information security management system. Requirements. Source: IP Paragraph.
4. Lukatsky A (2017) Ensuring information security of a modern university.
5. Volkov AV (2006) Providing information security in universities. Journal Information Security.
6. Boranbayev Askar, Mazhitov M, Kakhanov Zh (2015) Implementation of Security Systems For Prevention of Loss of Information at Organizations of Higher Education. The proceedings of 2015 12th International Conference on Information Technology -New Generations, USA, pp. 802-804.
7. Boranbayev SN, Tasmagambetov OK, Baidildina M (2016) Methods for safety and reliability of information systems. Herald of ENU 2: 33-40.
8. Boranbayev SN, Tasmagambetov OK (2016) Forms and methods of integration of information systems for law enforcement of Kazakhstan. Herald of ENU 2: 26-32.
9. (2012) Law of the Republic of Kazakhstan on the National Security of the Republic of Kazakhstan. No. 527-IV.
10. (2015) Law of the Republic of Kazakhstan on Informatization. No. 418-V.
11. (2016) Government Regulations of the Republic of Kazakhstan On Approval of the Rules and Criteria for assigning of objects of information and communication infrastructure to critically important objects in the sphere of informatization. No. 529.
12. (2018) Order of the Minister of investments and development of the Republic of Kazakhstan On approval of the methodology and rules for carrying out the testing of the service program product, information and communication platform of "eGovernment", Internet resource of the state body and information system for compliance with information security requirements.