PRODUCTION ENGINEERING ARCHIVES 17 (2017) 25-28

PRODUCTION ENGINEERING ARCHIVES

ISSN 2353-5156 (print)
ISSN 2353-7779 (online)

Exist since 4th quarter 2013
Available online at www.qpij.pl/production-engineering-archives

Analysis of Information Security Threats for Developing DLP-systems

Ekaterina Polozova[1], Nataliia Anashkina[2]

[1] PhD. Student in Information Security, Information Technology and Data Protection Department, the Ural State University of Railway Transport, Kolmogorov Street, 66, Yekaterinburg RUSSIA, e-mail: polozova.ekat@gmail.com

[2] PhD. in Linguistics, Logistics specialist, Associate Professor of Foreign Languages and Intercultural Communication Department, the Ural State University of Railway Transport, Faculty of Economics and Administration, Kolmogorov Street, 66, Yekaterinburg RUSSIA.

Article history
Received 20.07.2017
Accepted 14.12.2017
Available online 31.01.2018

Keywords
Data Leak Prevention (DLP)
information security
threat model
automated system

Abstract
The motivation of investigation is explained by the problem of keeping organisations' information and private ones secure. One reason for this is insufficiency of information protection systems, and another – vulnerability in such kind of systems. The article is devoted to defining and analyzing the types and sources of information security threats for an automated system. It can be useful for developing the model method, having the purpose of detecting and further preventing of hazards. The safeness of Data Leak Prevention (DLP) system itself is also under investigation. The analysis was carried out by an expert method with system analysis. A DLP system was considered, on the one hand, as a way of information protection to prevent information leakage, and on the other hand, as an object of protection which is vulnerable to threats of information security. The presented threat model includes the sources of threats, divided into three large groups: anthropogenic, technogenic and spontaneous; and types of threats: intentional and unintentional.

1. Introduction

At present, one of the main problems in the world is the information security.

According to the InfoWatch Analytical Center Report (2016) on the investigation of incidents related to safeness of limited access information in Russian commercial and non-commercial companies, government agencies and organizations in 2016 the picture of data leaks is rapidly approaching the global picture. This is due to the similarity of security objects (the types of data used), the growth of the value of information and the increase in the number of data transmission channels. All the incidents were published in the media, blogs, and social networks.

There are some key facts:

• In 2016, the media reported 213 cases of information leakage from Russian companies and government agencies, which is 14% of the number of data leaks around the world.

• Most often in Russia, personal data and payment information disclose. These types of data account for 80% of the leakage that occurred in 2016.

• In 68% of cases, employees of companies were found guilty of information leakage, in 8% of cases - organizational administrative staff.

• In 2016, in Russia, the largest share of leakage fell on the network channel and paper documentation - 64% and 26% respectively.

Requirements, methods, information security systems, hardware and software products for information protection, etc. are being intensively developed. Relatively recently, the products to protect information - DLP-systems did appear.

The functional of DLP-systems is continuously growing. These systems cover some of the threats, but constantly new threats emerge and DLP systems themselves can be attacked. Documents for many systems are formed on the basis of the scheme (GRUDZIEŃ Ł., HAMROL A. 2016): applicability, comprehensiveness, accuracy, conciseness, consistency correctness and currency, to describe process information in a comprehensive manner. Information safety is becoming a very important part to most organizations due to current trends in information transfer, especially in the fact of a borderless and vulnerable world (SHAMALA P., ET AL. 2017). Existing methods DLP give the ability to prevent data leak-

age by either looking for specific keywords and phrases or by using various statistical methods (KATZ G., ET AL. 2014; XU CH., ET AL. 2017). The Data Leakage Prevention (DLP)-systems also include solutions that analyze, monitor and control information usage across computing systems (AHMAD A., ET AL. 2014; ALNEYADI S., ET AL. 2016; ZYWIOŁEK J. 2016).

This issue is quite urgent, because vulnerability and threats in this kind of systems can lead to sufficient damage not only for a particular individual, but also for the whole organization.

2. Basic concept

Data Leak Prevention (DLP) is a technology used to prevent the leakage of confidential information from the information system as well as from technical devices (software or hardware) to the outside. Other terms such as Data Loss Prevention (DLP), Data Leakage Protection (DLP), Information Protection and Control (IPC), Information Leak Prevention (ILP), Information Leak Protection (ILP), Information Leak Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion Prevention System (EPS) are also used to refer to this technology. Among all these terms there is no name for the technology which is the most popular or which can be called the basic term.

An effective approach to protection from information leaks from computers begins with the use of context control mechanisms - control of data transfer for specific users, depending on the data formats, types of interfaces and devices, network protocols, the direction of transmission, time of day, etc. (COMPARISON LEAKAGE PROTECTION SYSTEMS (DLP) PART 1 2014).

However, in many cases, a deeper level of control is required, e.g., checking the content of the transmitted data for the presence of confidential information in circumstances where data transmission channels should not be blocked in order not to disrupt production processes, but individual users are included in the "risk group" because they are suspected of being involved in violations of corporate policy. In such situations, in addition to contextual control, the use of content analysis technologies is necessary to detect and prevent the transfer of unauthorized data, without interfering with the exchange of information within the scope of official duties (SULAVKO A. Y. 2014).

DLP-systems are built on the analysis of data streams that cross the perimeter of the protected information system. When an active component of the system is detected in this confidential information stream, the transmission of the message (packet, stream, session) is blocked (BORIDKO I. S., ET AL. 2013).

Below there is a diagram (Fig. 1), which describes the percentage of infringers of information security (COMPARISON LEAKAGE PROTECTION SYSTEMS (DLP) PART 2 2014).

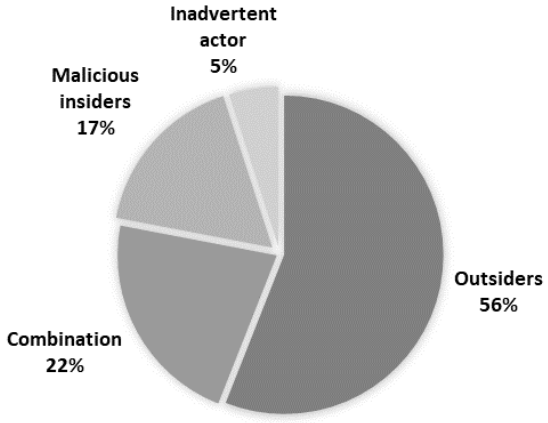

Fig 1. Cyber security event perpetrators, 2014

It can be seen from Figure 1 that the analysis may be carried out according to two parameters: the direction of threats (external or internal) and the intention presence (occasional and intentional). The diagram shows that most of the violators are external (56%) in comparison with pure internal violators – 17%. But internal violators can act in collusion. Among all the cases there are some, which occur unintentionally (5%). The main objective of DLP-systems, obviously, is to prevent the transmission of confidential information.

According to the international anti-virus company ESET (Slovakia) during a joint survey with FutureToday, the leading Russian consultant in the field of employer brand management (ESET PRESS-CENTRE 2014), the situation is as follows: most of the verified leaks (about 3/4) are not intentional, but occur because of errors, negligence, and carelessness of employees which makes leakages easier to detect.

The remaining leaks are connected with malicious intentions of operators and users of information systems. Obviously, insiders tend to overcome the defense of DLP-systems. The outcome of this struggle depends on many factors, and it is impossible to guarantee an absolute success in such a situation.

More than one third of employees at least once in their careers copied, deleted, or made public the confidential data of their former employers. 17% of respondents from this one third admitted that they had to destroy valuable documents, correspondence materials or software to harm the former employer.

13% of the respondents took away some working materials (for example, clients' database, plans, reports and other data) for subsequent sale or use at a new place of work.

About 4% of employees after the dismissal used the errors of the IT specialists of the former company; in particular, they went to work mail or continued to remotely visit corporate resources.

Another 4% of respondents openly took revenge on the former employer - they published corporate information (from financial documents to personal management data) in the Internet.

Finally, 62% of the survey participants never did anything like this, changing their place of work.

3. Results and discussion

To find a solution to the problem of keeping information secure, potential threats when building a model need to be detected and DLP system needs to be further developed which should be safe in itself. To gain the material for the research the situation in Organization X was analyzed. There was an attempt to build a threat model, which was divided into two parts:

• a group of threats concerned with an automated system, and DLP functions in relation to an automated system;

• a group of threats concerned with a DLP system itself.

The first group is related with the possibilities of a DLP-system in an automated system, from which threats a DLP-system can protect an automated system. The second group describes what kind of threats put at risk a DLP system itself. Accordingly, these threats can damage the automated system.

As a result, it turned out that 22 threats are relevant to the first group, 14 threats are actual for the second group. Also in this model, three types of threats' *sources* are indicated: anthropogenic, technogenic and spontaneous, and two types of *threats* are specified: intentional and unintentional.

Below there is a bar chart (Fig. 2), which describes a number of threats by source and type of threats for the automated system where DLP is installed and a bar chart (Fig. 3), which describes the number of threats by source and type of threats to which the DLP system is exposed.

To establish the development of a threat model, GOST R 51275-2006 "Data protection. Informatization object. Factors affecting the information. General provisions." was taken into consideration (GOST P 51275 2006). About 100 threats were analyzed. Not all the threats and factors that are listed in GOST R 51275-2006 are relevant. Expert method was used to highlight the current threats.

Software and hardware are indispensable components for ensuring the security of modern information systems. However, apart from this, there is physical, organizational, legislative protection of information. DLP-system is effective only in combination with the above mentioned protection measures.

Because of the fact that the human factor plays an important role in protecting information, first of all, it is necessary to properly instruct employees and teach them the basics of information on protection. In this case the threats caused by a user, system, as well as many information protection tools, is a subject to threats attacks itself. DLP-system was developed as a means of protecting information from internal threats and internal violators. It must be controlled so that when developing an information security system, it is necessary to cover all the current channels of information leakage. Having eliminated some threats, one may detect new threats. Therefore, it is necessary to constantly update the threat model. It is important to know that DLP-systems cannot fully protect the automated system. Moreover, the DLP-Errors or other unintended effects will decrease several times. When developing and implementing an information security system, it is necessary to take into account all current threats, from both the automated system and the DLP-system.

Threats to which the DLP system itself is exposed should be blocked by other methods of information protection, or the DLP system should be improved.

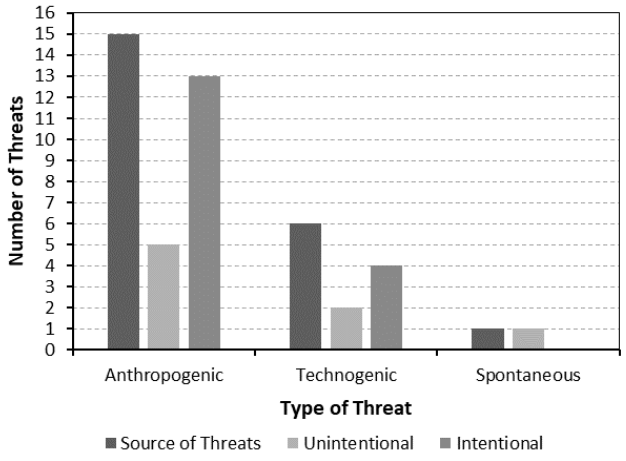

Fig. 2. Number of actual threats by source and type of threat (automated system)

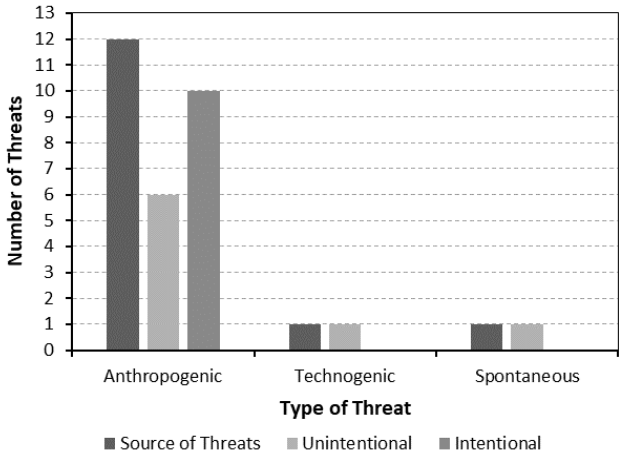

Fig. 3. Number of actual threats by source and type of threat (DLP-system)

Additionally, it is important to monitor the actions of employees. Another point should be taken into account, that is spying on employees with the help of this program can negatively affect the morale of the team.

DLP system does not allow to counteract leaks of information resulting from theft or loss of equipment and media, external hacking of networks and other actions are not covered by DLP policy.

4. Summary and conclusions

In the following paper–the basic concepts related to DLP systems were considered, general threats for DLP systems were presented, as well as the current threats both for the automated system on which the DLP system is installed and for the DLP system itself were identified.

The obtained results can serve as a basis for the development of DLP systems, as well as for the construction of an information security system that will use a DLP-system.

Reference

AHMAD A., BOSUA R., SCHEEPERS R. 2014. *Protecting organizational competitive advantage. A knowledge leakage perspective*. Computers & Security, Vol. 42, 27-39. DOI: 10.1016/j.cose.2014.01.001.

ALNEYADI S., SITHIRASENAN E., MUTHUKKUMARASAMY V. 2016. *A survey on data leakage prevention systems* Journal of Network and Computer Applications, Vol. 62, 137-152. DOI: 10.1016/j.jnca.2016.01.008.

BORIDKO I. S. ET AL. 2013. *DLP-systems: insider protection*, Security of information technology, 1, 82-84, ISSN: 2074-7128eISSN: 2074-7136.

COMPARISON LEAKAGE PROTECTION SYSTEMS (DLP) 2014. Part 1, URL: https: //www.anti mal-ware.ru/comparisons/data_leak_protection_2014_part1.

COMPARISON LEAKAGE PROTECTION SYSTEMS (DLP) 2014. Part 2, URL: https://www.anti-malware.ru/comparisons/data_leak_protection_2014_part2

ESET PRESS-CENTRE 2014. URL: https://www.esetnod32.ru/company/press/center/38-sotrudnikov-slivali-sekrety-eks-rabotodateley/.

GOST P 51275-2006. Data protection. information of the object. Factors affecting the information. General Provisions.

GRUDZIEŃ Ł., HAMROL A. 2016. *Information quality in design process documentation of quality management systems*. International Journal of Information Management, Vol. 36 (4), 599-606. DOI: 10.1016/j.ijinfomgt.2016.03.011.

INFOWATCH ANALYTICAL CENTER REPORT DATA LEAKAGE. Russia. 2016. URL: https://www.infowatch.ru/analytics/reports/17962.

KATZ G., ELOVICI Y. SHAPIRA B. 2014. *CoBAn. A context based model for data leakage prevention*. Information Sciences, Vol. 262, 137–158. DOI: 10.1016/j.ins.2013.10.005.

SHAMALA P., AHMAD R., ZOLAIT A., SEDEK M. 2017. *Integrating Information Quality dimensions into information security risk management (ISRM).* Journal of Information Security and Applications, Vol. 36, 1-10. DOI: 10.1016/j.jisa.2017.07.004.

SULAVKO A. Y. 2014. *Technologies of protection from inner threats of information security*, Bulletin of the Siberian State Automobile and Highway Academy.

XU CHANGBAO, ZHAO YANLONG, ZHANG JI-FENG, QI HONGSHENG 2017. *System Identification under Information Security*. IFAC-PapersOnLine, Vol. 50 (1), 3756–3761. DOI: 10.1016/j.ifacol.2017.08.477.

ZYWIOŁEK J. 2016. *The application of value stream mapping method for identifying basic drawbacks and reducing duration of information process in a company*, Production Engineering Archives, Vol. 11, No. 2, 36-39.

分析开发DLP系统的信息安全威胁

關鍵詞
数据泄漏防护（DLP）信息安全
威胁模型
自动化系统

摘要
调查的动机是由组织的信息和私人的安全问题来解释的。其中一个原因是信息保护系统不足，另一个原因是这种系统存在漏洞。本文致力于定义和分析一个自动化系统的信息安全威胁的类型和来源。这对于开发模型方法是有用的，其目的在于检测和进一步预防危害。数据泄漏防护（DLP）系统本身的安全性也在调查之中。分析采用专家方法进行系统分析。 DLP系统一方面被认为是防止信息泄漏的信息保护方式，另一方面被认为是一个容易受到信息安全威胁的保护对象。提出的威胁模型包括威胁来源，分为三大类：人为的，技术性的和自发性的;以及威胁类型：有意和无意。