Threats of leakage of confidential data and their influence on commercial activities

Романов Александр Сергеевич – студент Московского государственного лингвистического университета.

Аннотация: В данной статье рассматривается актуализация инцидентов утечки конфиденциальных данных, как одного из самых часто реализуемых видов угроз информационной безопасности. Приводятся базовые меры пресечения попыток хищения информации, и последствия утечек конфиденциальной информации. Характер и ценность похищаемой информации, позволяют утверждать о ее высокой ценности для злоумышленников.

Abstract: This article discusses the actualization of incidents of leakage of confidential data, as one of the most frequently implemented types of threats to information security. Basic measures are taken to prevent attempts to steal information, and the consequences of leaks of confidential information. The nature and value of the stolen information allows us to claim its high value for attackers.

Ключевые слова: Инсайд, конфиденциальная информация, политика безопасности, последствия утечек.

Keywords: Insider, confidential information, security policy, consequences of leaks.

Introduction

In 2018, the InfoWatch analytical agency conducted a series of studies to identify the most common types of information incidents that occur in organizations. According to research, the most valuable information for attackers is the personal data of users, 80 percent of the incidents were aimed specifically at obtaining personal data. [1] The main culprits of the incidents were employees of organizations.

These statistics are not new. Over the past decade, the tendency to steal confidential information of an organization by its employees has continued. In the article we will consider how these incidents happen and whether all of them can be considered as an attempt to insider activity.

Reasons for insider trading

Information leaks can be divided into two main groups: intentional and unpremeditated. Intentional data leakage comes from the desire of employees to sell the organization's confidential data, for personal gain or hostility to the organization's management. In the information exchange system, a person is the most unpredictable element, it is very difficult to predict his behavior and actions, therefore, as a result, it is not always possible to detect an attacker. The greatest threat insiders pose to the intellectual property of the company, which is its main asset.

According to the information provided by InfoWatch agency, the insider is most often a person aged 30 to 50 years [2], who is highly trusted in the organization. This level of trust allows a person to succeed in insider activity, because it allows to get access to various documents even not a high-ranking employee.

Several types of insiders can be distinguished depending on their behavioral archetype.

Curiosity. This species is characterized by a desire to learn and share confidential information. An employee may not have a desire to harm the organization, but posting and disseminating information on special thematic forums, on the Internet, and social networks allows third parties to receive the necessary information. [2]

Vengeance. The desire of this employee to steal and use information comes from personal problems within the organization. The most frequent cases include dismissal of an employee with the subsequent dissemination of confidential information. [1]

Self-serving. It is characterized by a desire to receive money for the leaked information. This archetype is the greatest danger to the organization, as it is able to remain unnoticed in the organization's system for a long time. [1]

Justice. As a classic example of this insider, you can cite Edward Snowden, who in January 2013 became the culprit in the dissemination of state secrets of the United States of America. The reasons were the desire to achieve justice, in the organization an employee who believes that its activities can lead to tragic consequences or violations is inclined to carry out insider actions. [2]

Regardless of the type of malicious insider, it is easiest to catch him using the DLP system. In any case, the leak of confidential information can cause a lawsuit, loss of customers and the reputation of the organization.

Measures to prevent information leakage

In order to prevent information leakage, it is necessary to fulfill the following conditions for ensuring information security [3]:

- Explaining employees the need for responsibility for information security. This responsibility should be included in the duties of employees, including responsibility for the implementation of information security policy requirements, resources, processes and security measures.
- Carrying out inspections of employees upon hiring, including checking the summary of recommendations, qualifications. Creating a complete image of the employee will allow you to set the level of power of attorney.
- One of the key clauses of the employment agreement should be an agreement on non-disclosure of confidential information.
- Information security requirements for an employee should be reflected in labor agreements. There should also be written responsibility for breach of security.

Raising staff awareness

An important role for ensuring information security is presented by users' awareness of security issues and their awareness of the rules of safe behavior. Awareness control, communicating security policy requirements, incorporating security requirements into job responsibilities are key points in employee training.

It is necessary to conduct training and control the knowledge of users on the following issues:

- organization security policy rules
- rules for choosing, changing and using passwords
- rules for gaining access to information system resources
- rules for handling confidential information
- procedures for reporting incidents, vulnerabilities, errors and software failures
- as well as other rules and procedures

Preventive measure

The organization must have an appropriate disciplinary process for security violators, including an investigation, elimination of the consequences of incidents and adequate measures of influence. [3]

When determining preventive measures, one should be guided by the provisions of the current legislation. The relationship between the employee and the employer and the corresponding liability for violation of the organization’s information security are regulated, first of all, by the Labor Code of the Russian Federation. In certain cases, it is possible to apply the provisions of the Code of Administrative Offenses and the Criminal Code.

Organization of the process of internal communication allows avoiding information leaks and its inappropriate use. It includes defining levels of access to information, control mechanisms, and functional roles.

Consequences of confidential information leakages

Despite the seemingly insignificant economic effect of information leakage, these incidents are the most economically disadvantageous for organizations. The company receives losses as a result of lawsuits filed by individuals affected by leaks, whose personal data were compromised, as well as fines from regulatory bodies involved in the protection of personal data at the state level.

In the same way leakage of internal documents of an organization lead to leakage of confidential data. Of course, they do not lead to direct losses in the form of fines or compensation, but they can seriously damage the reputation of the company that made such leaks. And a damaged reputation automatically means lost profit, as a number of potential customers or partners can change their preferences in choosing between several competing

companies, and the reason for such changes can be both the information that became public as a result of the leak, and the fact of such a leak of confidential data. Financial losses also depend on the position and nature of the data lost.

Conclusion

Thus, we can say that any information leak carries certain negative economic consequences for the company. The high probability of this incident, as well as high economic losses, make it possible to talk about information leakage in organizations as one of the main types of threats. Why evaluate the potential damage from information leaks? First of all, in order to understand what price the confidential information actually possesses by the organization, as well as to assess the benefits of implementing means of protection against information leaks. The benefit, of course, is when the cost of possible leaks is at least 2 times higher than the cost of introducing such a system. As practice shows, for the vast majority of companies the introduction of a DLP system is really advisable.

References

1. Главные утечки 2018 года [Электронный ресурс] // InfoWatch. URL: https://www.infowatch.ru/resources/analytics/digest/15203 © (Дата обращения: 29.10.2019).

2. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года [Электронный ресурс] // InfoWatch. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1 © (Дата обращения: 04.11.2019).
3. Барт Бэзенс, Ваутер Вербеке Fraud analytics using descriptive predictive and social network techniques: M., 2015. 437c.

{social}