Bushuev Anton
Student
Ural federal University
Russia, Yekaterinburg
Research advisor: Kovaleva Alexandra

MODERN METHODS OF PROTECTION AGAINST INSIDER THREATS

Abstract: *The most dangerous threats faced by organizations are insider attacks. Because insiders are aware of the structure of the system, handling insider attacks is the most important task in the modern world. The article is devoted to the problem of insider threats in the modern world. Questions explaining the essence of insider threats will also be considered.*

Keywords: *Information security, insider threat, insider, access control, multi-modeling.*

Бушуев Антон Олегович
Студент
Уральский Федеральный университет
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ОТ ИНСАЙДЕРСКИХ УГРОЗ

Аннотация: *Наиболее опасными угрозами, с которыми сталкиваются организации, являются инсайдерские атаки. Поскольку инсайдеры осведомлены о структуре системе, обработка инсайдерских атак - самая важная задача в современном мире. Статья посвящена проблеме инсайдерских угроз в современном мире. Также будут рассмотрены вопросы объясняющие суть инсайдерских угроз.*

Ключевые слова: *Информационная безопасность, инсайдерская угроза, инсайдер, контроль доступа, мульти-моделирование,.*

INTRODUCTION

Damage from insider threats was estimated at an annual average of $ 4.3 million per company across industries in the 2016 study, which does not include damage to the organization's reputation, loss of business, and decline in the company's value. Insider threats cause the greatest damage to the organization in terms of costs. All current trends point to an increase in the number of future incidents.

Proper management of authorization and privileged user access will be useful to reduce the risk of insider threats. Privileged identities can be controlled by access control mechanisms. In the access control mechanism, the main tasks are authentication and authorization. However, the password authentication mechanism is not sufficient to protect against potential intruders. Thus, it is necessary to determine effective methods of protection against insider threats.

DEFINITION

Insider threats can take many forms within an organization. These include those who steal sensitive or proprietary data, commit acts of violence in the workplace, or commit any other acts detrimental to the organization.

A common definition of insider threat is «a current or former employee, contractor, or other business partner who has or has had authorized access to an organization's network, system, or data and who intentionally (or unintentionally) exceeds or abuses that access to adversely affect the confidentiality, integrity, or availability of the organization's information or information systems» [1, c. 101].

Insiders are traditionally divided into traitors and, masquerades. A traitor is someone who authorizes access to an asset to perform some action that will cause damage to that asset. A person who acquires the identity of a legitimate user and commits a malicious act on behalf of a legitimate user is called masquerade [3, c. 158].

METHOD OF PROTECTION:

As insiders are treated as authorized users of the system, properly managing authorization and privileged user access will be helpful in reducing insider threats.

Privileged identities can be controlled by access control mechanisms. In the access control mechanism, the main tasks are authentication and authorization. However, the password authentication mechanism is not efficient enough. Thus, another integrated mechanism is often used (e.g. multi-level authentication schemes, biometrics, etc.). However, the above methods are not sufficient to provide the required level of protection.

Therefore, to solve this problem, the program «The Scientific advances to Continuous Insider Threat Evaluation» was created, the purpose of which was to improve the methods of insider threat detection. The study found that the best way to detect insider threats is a multi-model prediction system. Its principle of operation is based on the theory of «wisdom of the crowd». In this system, several independent models were used, which predicted the possibility of implementing an insider threat, after which their results were compared and, on the basis of which a final decision was made. According to the results of the study, this model demonstrated the accuracy of predictions equal to 60% [1, c. 101-106].

Also, as an alternative, a different approach is being developed to authentication systems that are most susceptible to insider threats. To reduce the impact, an access control system based on the assessment of employee behavior was proposed, which does not request personal data of the employee to provide information, but the reason for this request, and then evaluates the previous actions of the user, determining the level of risk. Based on the risk, a decision is made whether or not to provide access to this information [3, c. 375-383].

CONCLUSION:

An insider is a current or former employee, contractor, or other business partner who has or has had authorized access to an organization's network, system, or data and who intentionally (or unintentionally) exceeds or abuses that access to adversely affect the confidentiality, integrity, or availability of the organization's information or information systems. As a rule, they are divided into traitors and masquerades. Methods of protection against insider threats are often reduced to the prediction of

insider attacks, which is well suited multi-model system, or advanced specialized systems based on risk assessment.

REFERENCES

1. David P. Brown. Improving Insider Threat Detection Through Multi-Modelling/Data Fusion [Текст] / David P. Brown// Procedia Computer Science – 2019. - № 153. – С. 100-107.

2. Abdulaziz Almehmadi and Khalil El-Khatib. On the Possibility of Insider Threat Prevention Using Intent-Based Access Control (IBAC) [Текст] / Abdulaziz Almehmadi and Khalil El-Khatib // IEEE SYSTEMS JOURNAL, – 2017. - № 11. – С. 373-384.

3. B. Mahesh Babu. Prevention of Insider Attacks by Integrating Behavior Analysis with Risk based Access Control Model to Protect Cloud [Текст] / Mary Saira Bhanu// Procedia Computer Science – 2015. - № 54. – С. 157-166.