Martynov Artem Stanislavovich
Student
Engineering School of Information Technologies,
Telecommunications and Control Systems
Ural Federal University
Russia, Yekaterinburg
Research advisor: Kovaleva Alexandra

ENSURING DATA SECURITY IN ENTERPRISE NETWORKS

Abstract: *The article is about the approaches of providing data security in inner networks of corporations. Three approaches of providing Information Security (IS) in networks are represented and reviewed in the paper. Each method solves its own problem such as enterprise staff non-compliance to IS policies or managerial vulnerabilities in IS systems.*

Keywords*: Data Security, Information Security, Networks, Information Security Policies, Trust Models, Information Security Awareness, Graph-Based Method.*

Мартынов Артём Станиславович
Студент
Уральский федеральный университет
Россия, Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ В КОРПОРАТИВНЫХ СЕТЯХ

Аннотация: *В статье рассматриваются методы обеспечения безопасности данных во внутренних сетях компаний. В статье представлены и рассмотрены три метода обеспечивающих Информационную Безопасность*

(ИБ) в сетях. Каждый метод решает свои собственные проблемы безопасности, такие как: несоответствие поведения сотрудников Политикам Информационной Безопасности или управленческие уязвимости систем ИБ.

Ключевые слова: *Информационная Безопасность, Безопасность Данных, Корпоративная Сеть, Политика Информационной Безопасности, Модель Доверия, Программа Осведомлённости об Информационной Безопасности, Метод, основанный на Графах.*

Introduction

In modern world of information the problem of information security becomes more and more important, especially for organizations and corporations in their inner networks. Each year the number of cyber-crimes is increasing and one of the most common attack targets is enterprises – their data and software and most dangerous and common crimes provided by internal vulnerabilities of networks [1]. Therefore many companies search new effective methods of ensuring information security. In that variety of threats it is important to know approaches of information security, how they are realized, their advantages, disadvantages, etc. In this paper we review three Information Security (IS) Systems that provide security from internal threats such as human errors, staff malicious behavior, security system non-compliance to IS Policies etc.

Information Security Awareness Program

The Information Security Awareness (ISA) program – is the program that provides enterprise staff and customers knowledge about current IS policies of company and training to avoid cyber-threats, situations and accidents that may cause damage to enterprise data. There is a big variety of the ISA programs due to fact that every big company creates their own ISA program based on their IS policies, but some ISA programs are more effective than the others.

According to specialized literature, effective ISA program should continuously update according to Deming cycle (plan-do-check-act work cycle), therefore users have to periodically reminder about ISA program and changes in IS policy [2]. There are the following recommendations for effective ISA program:

- Media richness in ISA interventions;
- Customizing ISA interventions;
- Implementation of an iterative control and improvement process;
- Non-technocratic IS risk and threat communication;
- Feedback interventions;
- Enforcement of reflection and dialogue;
- Use of a role play.

For example, a good working bank ISA program is based on four weeks campaign with different themes and quizzes every week. This program is continuously improved by two-way connection IS-department and users [2].

Trust Models

The Trust systems – is the systems that provide evaluation of stakeholders before enterprise start to communicate with them to determine their trustworthiness. All trust models are divided on three groups: credential-based systems, reputation-based systems and trust in information resource (combination of credential-based and reputation-based models).

All these models should acquire to the list of attributes [3]:

- Context dependency;
- Non-transitivity;
- Non-monotonicity;
- Subjectivity;
- Uncertainty;
- Asymmetry;
- Temporal decay;
- QoS (quality of service) monitoring;
- Hierarchy;
- Credential validity;
- Feedback credibility;
- Feedback similarity.

At the current period the trust model that supports all attributes does not exist, therefore even when trust model positively evaluate stakeholders, there is the need of additional check to ensure their reliability.

Graph-Based Method

The Graph-Based method provides effective and formal management of IS systems to prevent or detect managerial vulnerabilities, specify IS policies and identify security threats. The methods represent entities of IS as groups of Graph that may analyze easily than tables or lists. The entities are represented as subnet, user, object, subject, Access rights and Security parameters. To evaluate IS systems by this method special graphs are created [4]:

- Physical Inter-Connection Graph shows the actual physical containment and connectivity of assets;
- User Inheritance Graph shows users or group users interconnections with each other and other entities;
- Access Control Graph represents enterprise access control policies;
- Composite Graph – it is combination of represented graphs to show relations between entities in security system.

Conclusion

In this paper we reviewed three methods of ensuring IS in enterprise systems. All three methods required big planning and continuous monitoring to provide proper level of Information security. These methods are suitable for big companies to design their information security systems.

REFERENCES

1. Andreea Bendovschi. Cyber-attacks – trends, patterns and security countermeasures, research article – URL: https://www.sciencedirect.com/science/article/pii/S2212567115010771

2. Stefan Bauer, Edward W.N. Bernroider, Katharina Chudzikowski. Prevention is better than cure! Designing information security awareness programs to

overcome users' non-compliance with information security policies in banks, research article – URL: https://www.sciencedirect.com/science/article/pii/S0167404817300871

3. Asmita Manna, Anirban Sengupta, Chandan Mazumdar. A survey of trust models for enterprise information systems, research article – URL: https://www.sciencedirect.com/science/article/pii/S1877050916305609

4. Asmita Manna, Anirban Sengupta, Chandan Mazumdar. A Graph-Based Approach for Managing Enterprise Information System Security, research article – URL: https://www.computer.org/csdl/proceedings-article/cube/2013/2235a137/12OmNAYXWGU