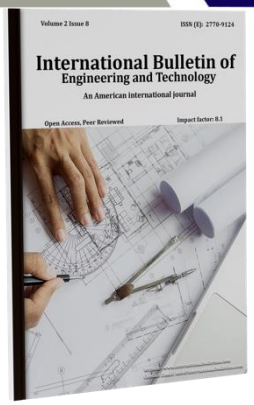

«STUDY AND DEVELOPMENT OF WAYS TO DETECT AND PREVENT CYBERATTACKS IN CORPORATE INFORMATION SYSTEMS NETWORKS»

Rakhmanov Shukhrat Yusupovich
Republic of Uzbekistan Termez State University Faculty of Sports Activities and Management Department of "Physical Education and Sports Games"
Rakhmanova Shakhzoda Shukhratovna
Co-Author:
https://doi.org/10.5281/zenodo.10604748

Annotation

The scientific article is timed to the current task of cybersecurity in advanced information developments. With the development of the number of cyberattacks and the complexity of their difficulty, the defense of information systems becomes a priority task for organizations and countries. The article presents the results of the study and development of methods for detecting and preventing cyberattacks in the networks of corporate information systems. The study includes testing of advanced threats and attacks, assessment of vulnerabilities of information systems, and development of algorithms for current detection of untrustworthy activity. The article also discusses machine learning technologies and artificial origin intelligence, applied for the improvement of the prediction and defense system's performance. The results of the study can be used in practical tasks of ensuring cybersecurity, which contributes to the protection of confidential information and ensuring the uninterrupted operation of information systems of organizations. The note emphasizes the importance of continuous updating of methods and technologies in the field of cybersecurity for effective defense of information assets.

Key words: information technologies, cyber security, cyberattacks, machine learning, detection methods, artificial intelligence, vulnerabilities, network protection, information systems.

Introduction

The modern world is completely and completely dependent on information technology. Collaborative information systems, which are the core of many organizations, preserve a huge amount of valuable data, covering economic information, individual customer data and business processes of firms. In connection with data, securing networks and data is becoming one of the values of advanced business and information technology.

1. The progress of cybersecurity hazards.

With the growth of digital modification, the level of cybersecurity hazards is constantly increasing. Cyber attacks are becoming more complex and sophisticated, threatening seemingly huge corporations, similar to small enterprises. Recent incidents, including data gains, malicious ransomware, and attacks on cloud services, underscore the need for continuous improvement of security systems.

2. Testimony and analysis of today's dangers

The first step in researching effective ways to detect and prevent cyber attacks is to analyze today's threats. This includes investigating a variety of attack patterns, including

phishing, application attacks, DDoS attacks, and more. Every type of attack requires unique methods of display and defense.

3.Development of algorithms and tools.

Academic research on cybersecurity is focused on developing new algorithms and tools that can detect unusual activity on the network and prevent attacks. Automotive teaching and artificial intelligence technologies are of paramount importance in this process, the reason being that they are able to consider the huge size of the data provided and identify unusual behavior.

4. Ensuring continuous defense.

Cybersecurity is a process that does not require long-term updating and improvement. Systematic forecasting of networks and systems, the resumption of antiviral databases and the use of exclusive security updates are the main nuances of providing continuous protection. In addition, the education of employees about the database and awareness of the latest dangers also play a decisive role

5. Note.

Ensuring cybersecurity in networks of collective information systems is a complex and multifaceted task. However, with long-term research, the development of new methods and technologies, and attention to training and updating security systems, companies can dramatically reduce the dangers and protect their valuable materials from cyber attacks. The solution to these problems becomes more important every day, and must maintain the importance and multiple defenses of information systems.

6. Use and implementation of methods

Describe specific methods and technologies that can be used to detect and prevent cyber attacks. Consider technologies such as behavioral mental testing, network intrusion detection mechanisms, machine learning and others. Give examples of successful implementations of their use in real corporate environments.

7. Trends in cybersecurity.

Discuss the hottest security trends and challenges. This has the ability to include an overview of the latest appearances of cyber attack, the evolution of dangers, as well as new developments in defense. Consider which cybersecurity nuances are becoming more relevant in real time, such as the defense of cloud systems and the Internet of things.

8. Regulation and compliance with generally accepted measures

Pay attention to cybersecurity laws and regulations, such as GDPR, HIPAA, and others. Specify what promises are being made to organizations in the field of data defense and what measures need to be taken to comply with these generally accepted measures

9. Conflicts and learning cases

See real cases of cyber attacks and conflicts in enterprise information systems networks. Analyze what detection and prevention techniques were (or were not) used in each case and what lessons can be learned from these conflicts.

10. The future of security.

Think about the future of cybersecurity and what challenges and demands are likely to emerge in the coming years. Consider likely technological innovations and educational trends in the field of information defense.

Problem solving.

Conclusion of the difficulty of detecting and preventing cyber attacks in corporate information systems networks urgently requires a comprehensive and systemic approach. Here are some steps and strategies that may help solve this problem:

1. Awareness of dangers and risks.

The first step is to become aware of all kinds of cyber threats that have a good chance of potentially affecting your information system. This includes phishing, malware, DDoS attacks, insider threats, and more. Assess which hazards are more relevant to your organization and what hazards they involve.

2. Developing a Cybersecurity Strategy.

Model a cybersecurity strategy that includes policies, procedures, and technologies for information defense. This strategy must include measures to detect, prevent and respond to cyber attacks

3. Implementation of modern technologies.

Invest in modern technologies and cybersecurity solutions. This has the ability to include the implementation of intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus programs, firewalls and other defense tools.

4. Employee Training and Awareness.

Teach employees the basics of safety and provide them with access to resources to detect and prevent hazards. Employees are required to know how to recognize phishing attacks and what cybersecurity practices should be followed when working with email and other systems.

5. Continuous monitoring and analysis.

Install monitoring and analysis systems that are capable of tracking down unusual activity on your network. Use machine learning and massive data analysis to identify anomalies.

6. Incident response.

Develop procedures for responding to cyber attacks. Decide in advance how you will respond to conflicts and what steps you need to take to minimize harm.

7. Systematic update and audit.

Periodically update your cybersecurity strategy and defense technology. Conduct security audits to detect weak spots and vulnerabilities in the system.

8. Compliance with Regulations and Laws.

Ensure that you comply with all appropriate generally recognized measures and laws relating to data cubersecurity and defense.

9. Cooperation with specialists.

If necessary, collaborate with external cybersecurity specialists and services to obtain additional expertise and support in ensuring the security of your information system.

10. Risk Management.

Review the risk management process to assess and manage cybersecurity risks in your organization. Solving the cybersecurity problem is an ongoing and multifaceted process that urgently requires attention and effort.

Cyber attacks

1. A large number of incidents over the years have led to significant harm in organizations and countries. Below are the most significant numbers in the situations: Cyber

attack on Equifax (2017): Equifax, 1 of the 3 largest credit bureaus in the US, was attacked by hackers, and as a result, the personal data of more than 143 million people were attacked. Existing regulation has had an impact on the privacy and security of the population.

2. WannaCry cyber attack (2017): This registration was sold with the introduction of the WannaCry ransomware virus and affected a large number of computer systems in more than 150 countries. Infected computers typically required payment in Bitcoin to unlock files. The attack affected a large number of organizations spanning England's National Health Service (NHS).

3. Sony Pictures Cyber attack (2014): In this case, hackers from the group Guardians of Peace hacked Sony Pictures Entertainment systems and stole a large amount of data, including emails and films. The attack was linked to the release of the film The Interview, which sparked political debate and incidents.

4. Cyber Attack on SolarWinds (2020): This registration is a difficult operation, resulting in very harmful software in the SolarWinds Orion program, which is used by almost all possible organizations and partner agencies. This opportunity allowed access to information in a large number of motivated organizations.

5. Cyber attack on a power plant in Ukraine (2015 and 2016): In 2015 and 2016, there were 2 cyber attacks on power plants in Ukraine, which actually led to a power outage costing 10 thousand. People. The attacks focused on political infrastructure and drew attention to the risks associated with political governance.

These attacks work, for example, in such a way that large companies increasingly become cyber threats, and then they increasingly influence various areas of life and business. In this concept, it is fundamental to take responsibility for your weight in gold and take appropriate measures to protect information and systems.

Cyber attacks are likely to occur in every country, covering Uzbekistan, and are likely to be targeted at all kinds of organizations, government agencies and personal data of people. In Uzbekistan, as in other countries, cyber attacks can have all sorts of purposes and methods. Below are some examples of cyber attacks related to Uzbekistan:

1. DDoS attacks on government and commercial websites: In Uzbekistan, DDoS attacks often occurred on the websites of government agencies, media and commercial organizations. These attacks could be carried out both by groups of hackers, for example, and by individual attackers.

2. Attacks on banking systems: Like many other countries, Uzbek banks still face cyber attacks. This has the ability to include attempts to hack bank accounts, as well as fraud with bank cards.

3. Spam and phishing attacks: Phishing attacks aimed at Uzbek users of email and public networks have a good chance of being carried out by both local and foreign hackers. These attacks are often aimed at obtaining their own information and credentials.

4. Cyber espionage: Cyber spies have every chance of collecting and collecting intelligence information related to Uzbekistan by hacking government or corporate networks.

It is important to note that cyber attacks can be carried out by hackers from different countries, and clearly identifying the origin of the attack can be a difficult task. The government of Uzbekistan, like almost all other states, is taking measures to protect cybersecurity and combat cyber threats.

To ensure personal cybersecurity, it is important to take precautions and implement data and network security methods, such as antivirus software, firewalls and intrusion detection systems.

Conclusion

The provided article discussed the significant nuances of advanced cybersecurity, covering the problems caused by cyber attacks and how to prevent them. Cyber attacks pose a serious threat to organizations and countries, and it is important to take measures to protect information systems and data.

In the article, you will notice that improving the way cyber attacks are detected and prevented is considered a critical task. This includes the development and implementation of modern cybersecurity technologies and strategies, the study of personnel in the field of cybersecurity and cooperation between organizations and countries.

In addition, proper advice has been offered:

1. Constantly updating software and patches to eliminate vulnerabilities.
2. Strengthening password security measures and multi-factor authentication.
3. Educate employees about cybersecurity and increase their awareness of potential hazards.
4. Development and implementation of a strategy for responding to conflicts in the field of cybersecurity.
5. International cooperation and exchange of information on cyber threats.

To conclude this article, I urge all organizations and countries to work actively to ensure cybersecurity and pay due attention to this task in order to minimize the dangers and harm caused by cyber attacks.

Cybersecurity is considered a necessary part of the advanced world, and ensuring it is a task that needs to be solved through common efforts.

Data is taken from various sources such as:

Journals: Journal of Cybersecurity, IEEE Transactions on Information Forensics and Security, as well as from sources of cybersecurity organizations: CERT (Computer Emergency Response Team), ISACA, and (ISC)^2

Ссылки и источники:

1.https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206
2.https://www.cert.gov.ru/en/
3.https://academic.oup.com/cybersecurity