ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 004.056.5 **doi: 10.32620/reks.2024.3.11**

Artem TETSKYI, Dmytro UZUN

National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine

INTRUSION DETECTION AND PREVENTION SYSTEMS AS A COMPONENT OF ENSURING COMPLIANCE WITH REGULATORY DOCUMENTS

Many financial institutions and payment solution providers must comply with PCI DSS (Payment Card Industry Data Security Standard). Such requirements are understandable because compliance helps reduce the risks of data leaks and financial losses associated with unauthorized access to card data. The presence of the PCI DSS compliance validation indicates that the organization has taken all necessary measures to protect data. An example web resource that must comply with PCI DSS regulations is considered. Implementation and testing of protection controls (measures) constitute an integral part of the compliance validation process. The methods used in intrusion detection and prevention systems have certain features that prevent the widespread and effective implementation of such systems. Thus, the focus of this study is intrusion detection and prevention systems, which are part of web application security systems. ***The goal*** *of this study is to identify the specific features of intrusion detection and prevention methods and provide recommendations for the combined use of the above methods. To achieve this goal, the following* ***tasks*** *are performed: identify the hierarchy/relationship of existing regulatory documents, according to which compliance validation can be performed; describe the basic provisions of PCI DSS certification; identify the protection systems that can be implemented to protect web resources from cyberattacks; to analyse the advantages and disadvantages of methods used in intrusion detection and prevention systems; and provide suggestions for improving the use of intrusion detection and prevention systems. Based on the defined* ***tasks****, the following* ***results*** *were obtained. It was found that the main problem with the intrusion detection signature method is the insufficiently fast updating of signature databases and the possibility of modifying known attacks such that known signatures are not used during the attack. The method of detecting anomalies is characterized by a large number of false positives at the initial stages of implementation; in this case, it is necessary to perform a thorough setup and training of the system based on conditionally safe user actions.* ***Conclusions.*** *The combined use of attack detection methods makes it possible to reduce the number of errors of the first and second types, which indicates the effective use of protection tools. Web resources that provide such protection can be certified if other conditions of the regulatory document are met.*

Keywords: *cybersecurity; protection systems; intrusion detection; intrusion prevention; compliance validation; regulatory documents, web application security.*

Introduction

Cybersecurity of web applications has become critical in a world in which digital technologies are ubiquitous throughout human life. With the growth of online transactions and electronic payments, financial institutions and payment solution providers are facing unprecedented threats related to cyberattacks [1]. In the conditions of constant technological development, criminals use increasingly sophisticated methods to gain access to sensitive data, which emphasises the need for reliable protection systems, e.g., intrusion detection and prevention systems (IDS/IPS) [2]. These systems provide early warning of potential threats and active protection against unauthorised access, which is an important element of an effective cybersecurity strategy [3].

An industry certificate can be both a guarantee of customer trust and a mandatory requirement for partners. Examples of such standards are HIPAA (Health Insurance Portability and Accountability Act) for healthcare and PCI DSS (Payment Card Industry Data Security Standard) for the banking sector [4, 5]. PCI DSS compliance validation is a key aspect of payment card processing organisations. The proposed standard contains a set of requirements designed to reduce the risks of data leaks and financial losses associated with cybercrime. Compliance with PCI DSS shows that the organisation has taken all necessary measures to ensure the security of its customers' data, which increases the level of trust on the part of consumers. PCI DSS-certified websites often gain a competitive advantage in the marketplace because data security becomes an important choice for users [6].

One of the main tasks in the PCI DSS compliance validation process is the implementation and testing of intrusion detection and prevention systems [7]. These systems help not only detect malicious access attempts, but also automatically respond to such attempts, thus minimising potential consequences. Intrusion detection approaches have their own peculiarities and challenges. For example, traditional signature methods require constant updating of the signature database, which can be problematic in the case of rapidly changing attacks. On the other hand, anomaly detection methods, although they can be more effective in recognising new threats, often face a high rate of false positives, which requires careful tuning and training of the system based on user behavior [8, 9].

Within the framework of this paper, the features related to the implementation of intrusion detection and prevention systems, which are an integral part of the PCI DSS compliance validation process, are considered. An analysis of modern regulatory documents regulating compliance validation will allow us to understand how to properly integrate protection tools into web applications to satisfy security requirements.

The goal of this study is to analyse the peculiarities of intrusion detection methods and provide recommendations for the combined use of the above methods. To achieve this goal, the following tasks are performed:

1) to identify the hierarchy/relationship of existing regulatory documents, according to which compliance validation can be performed;

2) describing the basic provisions of PCI DSS certification; and

3) identify protection systems that can be implemented to protect web resources from cyberattacks;

4) to analyse the advantages and disadvantages of the methods used in intrusion detection and prevention systems;

5) to provide suggestions for improving the use of intrusion detection and prevention systems.

1. Analysis of critical infrastructure protection based on legislative documents, standards and practices

In today's world, the protection of critical infrastructure has become a priority task for states and organizations. This is explained by the growing number of cyberthreats and the need to ensure uninterrupted operation of vital systems, such as energy, transport, healthcare, and finance. Together, legislation, standards, and industry decisions form a comprehensive cybersecurity strategy.

Legislative documents, including acts of Congress, provide a framework for critical infrastructure protection, but they are general in nature. They provide a framework and direction for the formation of policies in the cybersecurity field, and specific decisions are left to the discretion of the executive authorities.

An example is the Homeland Security Act, which provides a framework to protect key systems [10]. This law, like many similar acts, does not contain detailed technical instructions but defines strategic priorities and political guidelines. As a result, standards and guidelines that are applied in practice are created on the basis of legislative acts. The main role of legislation is to provide a legal basis on which further normative acts can be built.

Executive regulations, such as guidance documents from the US National Institute of Standards and Technology (NIST), provide specific guidelines for cybersecurity implementation. For example, the NIST Cybersecurity Framework offers practical approaches to assessing risks and implementing cybersecurity policies [11].

The NIST Framework is based on three main principles: risk identification, protection, monitoring, and response. Systems must be constantly monitored for potential attacks and must be capable of rapid response. An important aspect of the NIST Framework is that it offers a framework for organizations regardless of their size or industry, allowing them to tailor security measures to their needs. This approach ensures the flexibility and universality of the standard [12].

One of the strengths of the NIST Framework is its alignment with international standards, particularly ISO 27001, which also emphasizes risk management and information protection [13]. Both standards have similar principles, in particular information security management through risk analysis and the implementation of measures to minimize them.

ISO 27001 is an international standard widely recognized in various countries around the world. Organizations that seek to work in the global market or cooperate with international partners often focus on this standard to ensure the compatibility of their systems with the requirements of other countries.

The importance of the NIST Framework is that it can serve as a guide for organizations wishing to meet both national and international requirements. This facilitates the integration of global approaches into cybersecurity, which is critical in today's world.

In addition to general standards, industry documents set specific requirements for information protection in individual sectors of the economy. Examples of such standards include the HIPAA for healthcare and PCI DSS for the banking sector. These standards extend the requirements of the NIST Framework and legislative acts, adapting them to the needs of specific industries. HIPAA is focused on the protection of medical data,

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

and it requires medical institutions to strictly control the confidentiality of patient information. Medical facilities are required to implement technical and organizational measures to reduce the risk of unauthorized access or data loss. The PCI DSS is a standard designed to protect user data in the financial sphere, particularly during payment transactions. This includes detailed requirements for the security of storage, transmission, and processing of payment cards [14]. This standard will be considered in more detail.

Industry standards work as additional mechanisms to ensure cybersecurity, considering the specifics of data processing in various sectors [15].

In addition to legal requirements and standards, IT companies implement several technical solutions to ensure cybersecurity. Both organizational measures and specific tools are used to monitor and protect network activities. Another important approach is the use of Secured SDLC (secured software development life cycle), which protects at all stages of creating a software product [16].

The structural connection of the listed provisions is illustrated in Figure 1.

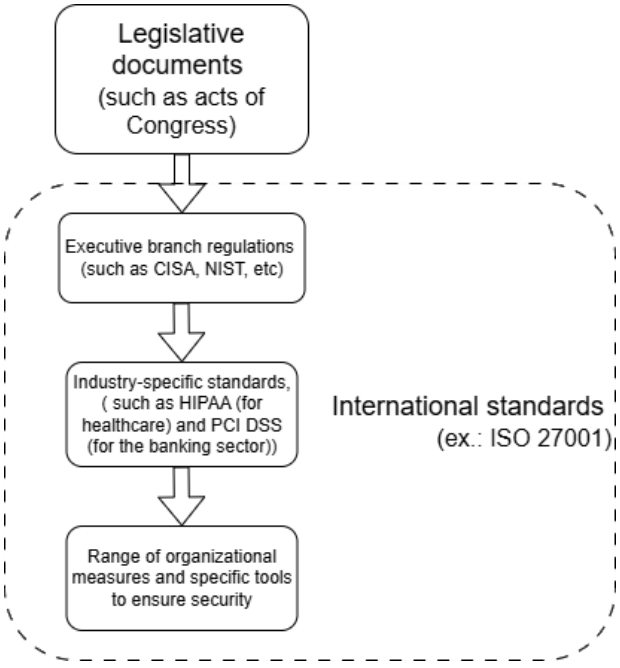

Fig. 1. Relationship of documents

Despite the effectiveness of the listed tools and approaches, organizations often face the problem of "compliance" – that is, compliance with regulatory documents. Sometimes, this aspect becomes too bureaucratic and can be perceived as a burden. Companies often invest resources in formal compliance instead of focusing on real security.

2. Basic provisions of PCI DSS compliance validation

There is a practice of PCI DSS certification, which is formally called PCI DSS compliance validation. Although many use the term "certification" informally, it is important to understand that the PCI Security Standards Council does not issue certificates in the traditional sense.

The process is for an organization to demonstrate compliance with PCI DSS through a compliance assessment that can be conducted by professionals such as

1. Qualified Security Assessor: qualified auditors who check companies' compliance with PCI DSS requirements.

2. Internal Security Assessor: Internal specialists from companies with relevant knowledge for independent assessment.

3. Self-assessment Questionnaire: For some companies, self-assessment is possible when a business fills out a compliance questionnaire.

After successfully passing the assessment, the company receives a documentary confirmation of compliance (for example, Attestation of Compliance) or a compliance report.

The PCI DSS standard contains 12 main requirements that can be divided into six main categories.

The first category involves building a secure network. This includes installing and maintaining network firewalls and configuring systems to protect card data.

The second category covers card data protection, which includes encryption and secure storage of sensitive information.

The third category requires a vulnerability management system that regularly updates software and monitors existing threats.

The fourth category concerns access control, which involves restricting access to data based on a user's role.

The fifth category covers network monitoring and testing, which includes log maintenance and regular analysis.

The sixth category deals with security policies, which involve training staff and developing procedures for handling card data.

A requirement of PCI DSS is the implementation of a comprehensive protection system. This system should include not only physical measures, such as access control to servers and other equipment, and software solutions capable of detecting and preventing unauthorized access to data. In this context, intrusion detection and prevention systems have become an

integral part of the organization's security architecture. Defense systems can be tested using penetration testing [17]. Similarly, security testing of systems that manage access to specific resources, including logical integrated circuits, can be performed[18]. The unique identifier of each microcircuit element in a certain board can be used to solve security problems [19].

IDS/IPS systems play a critical role in detecting suspicious activities and anomalies that may indicate cyberattacks. They analyze traffic passing through a network and detect potential threats based on established rules and algorithms. This allows quick response to hacking attempts, thereby reducing the risks of data leakage and financial and reputational losses.

PCI DSS compliance validation is a process that requires constant attention and effort from the company. After validation, the organization undertakes to maintain the established standards, which include updating the protection systems in accordance with new threats and requirements. This involves regular training of personnel, validation of existing security systems, and adaptation to changes in the technological environment.

There are four levels of PCI DSS compliance, which are determined by the number of transactions processed during a year [20] .

3. Protection systems that can be implemented to protect the web resource from cyberattacks

An IDS analyzes network traffic or logs to detect suspicious activity or potential attacks. However, reporting such incidents and does not take active measures are taken to prevent them.

IPS works similarly to IDS but with a proactive approach. In addition to detecting threats, the system can automatically take measures to avoid them, such as blocking suspicious traffic or changing network configuration.

These tools work on one or more devices (servers) and can also cover the entire network.

IDS/IPS are often integrated with security information and event management (SIEM) systems, providing centralized incident management and data analysis to detect complex threats (Figure 2) [21].

Interactions between IDS/IPS and filtering tools for spam, phishing emails, malware, and antivirus software are of great importance to ensure cybersecurity. The joint use of these technologies makes it possible to improve the effectiveness of threat detection and attack prevention [22].

Spam filtering detects and blocks unwanted emails that may contain malicious links or attachments. IDS/IPS can work against such systems through email header analysis and traffic analysis. An IDS can detect anomalies or inconsistencies in email headers that are typical of spam or malicious emails and report such anomalies to the spam filtering system to block such messages. IPS can monitor abnormal network activity caused by mass spamming or interactions with spam servers and automatically block such connections [23].

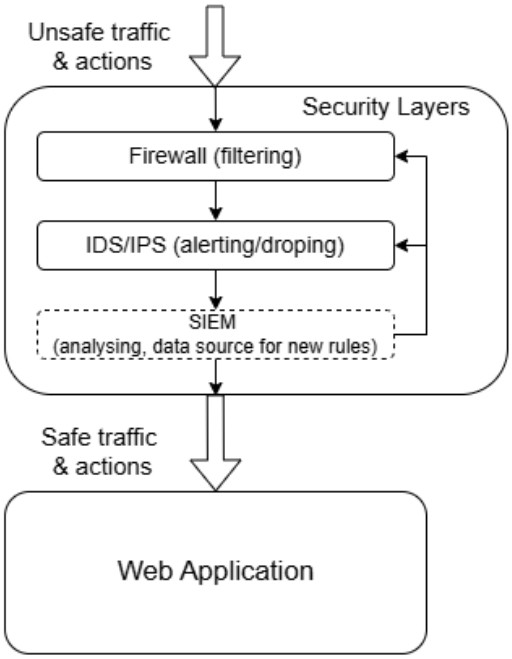

Fig. 2. Security layers architecture

Phishing attacks are aimed at deceiving users to steal their confidential data (passwords, payment information, etc.). IDS/IPS supports anti-phishing tools by monitoring phishing URLs and analyzing behavior patterns. IDS can detect URLs associated with phishing attacks by analyzing HTTP/HTTPS requests and comparing them to known databases of malicious sites. IPS may block such requests based on the detected URLs. IDS can analyze suspicious user behavior or requests targeting phishing resources and notify other systems to prevent attacks [24].

Malware can be spread via the Internet, emails, or USB drives. IDS/IPS can interact with antivirus programs and other antimalware systems by analyzing suspicious traffic and scanning traffic for malicious files. IDS can detect signs of malware being downloaded or distributed over a network (for example, unusual traffic patterns or connections to known malicious servers). IPS can automatically block such downloads or isolate suspicious traffic. IDS can integrate with deep file analysis systems (for example, antivirus systems or sandbox technologies) to analyze the contents of files passing through a network. If

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

malicious files are detected, IPS can block their transfer [25].

Antivirus software is capable of detecting and neutralizing known malware on endpoints (computers, servers). IDS/IPS can improve the effectiveness of antivirus protection by sharing threat data and blocking attacks in real time. IPS can block traffic from infected devices without waiting for an antivirus program to find and remove the malware, thereby reducing the risk of infection spreading further across the network.

4. Analysis of intrusion detection methods

Intrusion detection and prevention systems are critical elements of cybersecurity, and their effectiveness is strongly dependent on the methods used to detect threats. Two main principles of the functioning of these systems can be distinguished: the signature method and anomaly detection method. The signature method is based on previously known signatures of attacks, which allows accurate identification of threats but limits the possibility of detecting new or modified attacks. In turn, the method of detecting anomalies can detect unusual patterns in the behavior of the network, but is often accompanied by a high level of false positives [26].

Among the main advantages of the signature method, it is worth noting its high accuracy in cases where a threat is already known. This method can be easily implemented in existing security systems due to its simple configuration. However, its disadvantages include the limitation in detecting new attacks that do not have fixed signatures and the risk of modification of known attacks that can bypass this protection. Delays in updating the signature database can also affect the timeliness of responding to new threats [27].

In contrast, anomaly detection is a powerful tool for detecting new and sophisticated attacks because it is not limited to predefined signatures. However, its use is often complicated by a high number of false positives, which requires careful adjustment and training of the system. This can be a significant barrier to its effective application under real conditions [28].

It is important to note that combining both methods can lead to optimisation of protection, because each of them compensates for the shortcomings of the other. The integration of new technologies, such as machine learning, can significantly improve anomaly detection processes, which allows systems to adapt quickly to new threats. Using threat and vulnerability data aggregators can be an effective source for IDS training because it increases the accuracy of threat detection and reduces the number of false positives.

5. Recommendations for the use of intrusion detection methods

In an ideal use case, the probability of errors of the first and second types should be close to zero;, that is, all malicious requests should be blocked, and legitimate traffic should not be blocked. In the first case, there are risks of financial losses due to data leakage. In the second case, the risks of financial losses are caused by possible lost profits when a commercial web resource (for example, an online store).

The combined use of both intrusion detection methods described in the previous section is advisable. In this case, it is possible to exploit the advantages of both methods.

Training on conditionally normal traffic is the key to the correct anomaly detection system. An intrusion detection system collects data from various sources, such as network traffic, system logs, user activity data, transactions, and other metrics. The proposed system examines historical data to determine what is considered "normal" behavior for a particular environment. This may include traffic regularity, request types, and user activity hours. When the system analyzes new data, it compares it to a defined baseline of normal behavior. If significant deviations are detected, the system marks them as potential anomalies. This may include, for example, sudden increases in traffic, unusual requests to the database, or attempts to access resources at unusual times. An example of anomalous user behavior could be only access to certain scripts, while there will be no access to images or other static files.

Indicators for analysis should be configured according to the system functionality. In practice, it is difficult to compare two intrusion detection systems that use the anomaly detection method, because even with the same set of indicators, these systems are trained on different data.

6. An example of Suricata intrusion detection system

Suricata is a multi-threaded IDS/IPS system capable of detecting intrusions and other malicious activities in real time and offers powerful security monitoring capabilities. Suricata supports various output formats and can be integrated with other security tools, providing a flexible solution for network security [29].

The system is based on the creation of user rules, which allow the intrusion detection system to adapt to the specific needs of the network and detect specific threats and suspicious activities.

Keywords in the rule body include a message describing the rule to display in logs, a pattern to search for in traffic, a unique rule identifier, rule version, attack

type classification, rule priority, flow direction, regular expressions, and thresholds to avoid redundant rule triggering. The other components of the rule are the action, protocol, and recipient and sender IP addresses. Suricata provides the ability to work as an IDS using the "alert" action, in IPS mode the "drop" action is used.

Examples of the rules are shown in Table 1, as well as the generation of traffic from one machine (Figure 3) and the detection of this traffic on another machine (Figure 4).

Table 1

Examples of custom commands for detecting DoS attacks

Name	Command for filtering
Rule for HTTP DoS/DDoS attack	alert http any any -> any any (msg:"Potential HTTP DoS/DDoS attack detected"; flow:established,to_server; content:"GET"; http_method; threshold:type threshold, track by_src, count 100, seconds 1; classtype:attempted-dos; sid:1000001; rev:1;)
Rule for packets that only open TCP connections	alert tcp any any -> any any (msg:"Potential SYN Flood attack detected"; flags:S; flow:stateless; threshold:type threshold, track by_dst, count 100, seconds 1; classtype:attempted-dos; sid:1000002; rev:1;)

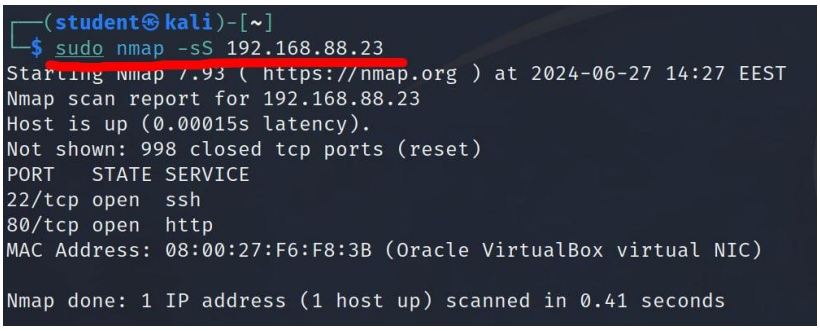

Fig. 3. Generation of suspicious traffic

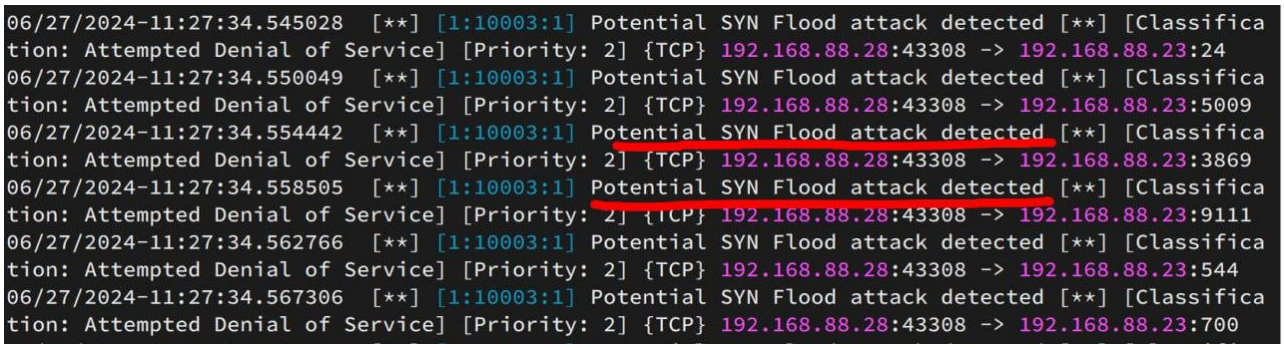

Fig. 4. Detection of suspicious traffic

7. Discussion

Intrusion detection systems have not been widely adopted for several reasons. First, a high false positive rate often creates additional difficulties for the administrator responsible for ensuring security. When a system routinely alerts to threats that are actually suspicious events, alert fatigue occurs. As a result, important messages can be ignored, which reduces the overall system efficiency.

Second, correct IDS settings require considerable effort. Systems require extensive training and constant monitoring to correctly identify what is considered normal behavior. This may require the involvement of highly skilled professionals, which is often a challenge for organizations with limited budgets.

In addition, with the development of new threats and attacks, traditional IDS systems often do not have time to adapt to new conditions. Many of these methods present problems with scalability, which complicates their implementation in large and complex networks. This is particularly relevant for companies that are growing rapidly or are facing various technological changes. These factors make the widespread adoption of IDS systems challenging for many organizations, despite their importance in the overall cybersecurity landscape and the need for security certification.

Improving the efficiency of IDS/IPS systems will not only improve the overall security of web applications and servers and provide more reliable protection against modern and constantly evolving cyberattacks.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Conclusions

Some existing normative documents, according to which compliance validation can be carried out, are considered, and their hierarchy is shown.

The main provisions of the PCI DSS standard used for payment card data storage and processing systems are considered.

The components of a protection system that can be implemented to protect a web resource from cyberattacks are considered.

The advantages and disadvantages of methods used in intrusion detection and prevention systems are analyzed. It was found that the main problem with the intrusion detection signature method is the insufficiently fast updating of signature databases and the possibility of modifying known attacks such that known signatures are not used during the attack. The anomaly detection method is characterized by a large number of false positives at the initial stages of implementation; in this case, more careful tuning and training of the system on conditionally safe user actions will help reduce the number of false positives.

Proposals are provided for the combined use of signature intrusion and anomaly detection methods. Thusway it's possible to take advantage of both types of detection.

Further research will be devoted to the following areas: (i) experimental investigations into the effectiveness of intrusion detection tools based on known rules that can identify common attacks; (ii) studies into the possibilities of using machine learning tools to detect modified attacks; (iii) research into the possibilities of using automated vulnerability scanners under the conditions of operation of intrusion detection systems at the scanning object.

Contribution of authors: analysis of PCI DSS provisions, analysis of protection systems, draft writing, preparing of references – **Artem Tetskyi**; analysis of regulatory documents, integration of protection systems, rules and examples of using Suricata, review and editing – **Dmytro Uzun**.

Conflict of interest

The authors declare that they have no conflict of interest related to this research, whether financial, personal, authorship, or otherwise, that could affect the research and its results presented in this paper.

Financing

This research was conducted without financial support.

Data availability

The manuscript contains no relevant data.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods in their work.

All authors have read and agreed to the publication of the finale version of this manuscript.

References

1. Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M. & Dawodu, S. O. CYBERSECURITY IN BANKING: A GLOBAL PERSPECTIVE WITH A FOCUS ON NIGERIAN PRACTICES. *Computer Science & IT Research Journal*, 2024, vol. 5, no. 1, pp. 41-59. DOI: 10.51594/csitrj.v5i1.701.

2. Ashoor, A. S., & Gore, S. Difference between intrusion detection system (IDS) and intrusion prevention system (IPS). *Advances in Network Security and Applications: Proceedings of 4th International Conference*, CNSA 2011, Springer, 2011, vol. 4, pp. 497-501. DOI: 10.1007/978-3-642-22540-6_48.

3. Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. A systematic literature review on the cyber security. *International Journal of scientific research and management*, 2021, vol. 9, no. 12, pp. 669-710. DOI: 10.18535/ijsrm/v9i12.ec04.

4. Moore, W., & Frye, S. Review of HIPAA, part 2: limitations, rights, violations, and role for the imaging technologist. *Journal of nuclear medicine technology*, 2020, vol. 48, no. 1, pp. 17-23. DOI: 10.2967/jnmt.119.227827.

5. Shabina, Ali, R. F., Jahankhani, H., Siddiqi, Y., & Hassan, B. Ensuring Securing PII Data in the AWS Cloud: A Comprehensive Guide to PCI DSS Compliance. Cybersecurity and Artificial Intelligence: *Transformational Strategies and Disruptive Innovation*, Springer, 2024, pp. 185-216. DOI: 10.1007/978-3-031-52272-7_8.

6. Williams, B., & Adamson, J. *PCI Compliance: Understand and implement effective PCI data security standard compliance*. CRC Press, 2022, 334 p. DOI: 10.1201/9781003100300.

7. Azeez, N. A., Bada, T. M., Misra, S., Adewumi, A., Van der Vyver, C., & Ahuja, R. Intrusion detection and prevention systems: an updated review. *Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019*, 2020, vol. 1, pp. 685-696. DOI: 10.1007/978-981-32-9949-8_48.

8. Masdari, M., & Khezri, H. A survey and taxonomy of the fuzzy signature-based intrusion detection systems. *Applied Soft Computing*, 2020, vol. 92, article no. 106301, pp. 1-19. DOI: 0.1016/j.asoc.2020.106301

9. Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. Machine Learning for Anomaly Detection: A Systematic Review. *IEEE Access*, 2021, vol. 9, pp. 78658-78700. DOI: 10.1109/ACCESS.2021.3083060.

10. Haughton, S. A., & Romaniuk, S. N. Civil Liberties and Homeland Security. *The Handbook of Home-*

land Security, CRC Press, 2023, pp. 525-531. DOI: 10.4324/9781315144511-73.

11. White, G. B., & Sjelin, N. The NIST cybersecurity framework. *Research Anthology on Business Aspects of Cybersecurity*, IGI Global, 2022, pp. 39-55. DOI: 10.4018/978-1-6684-3698-1.ch003.

12. Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., de Sousa Júnior, R. T., & Nunes, R. R. Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology. *IEEE Access*, 2021, vol. 9, pp. 129605-129618. DOI: 10.1109/ACCESS.2021.3113178.

13. Alshar'e, M. Cyber security framework selection: Comparision of NIST and ISO27001. *Applied computing Journal*, 2023, pp. 245-255. DOI: 10.52098/acj.202364.

14. Hassan, M. A., Shukur, Z., & Hasan, M. K. An efficient secure electronic payment system for e-commerce. *Computers*, 2020, vol. 9, no. 3, article no. 66, pp. 1-13. DOI: 10.3390/computers9030066.

15. Sobb, T., Turnbull, B., & Moustafa, N. Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, 2020, vol. 9, no. 11, article no, 1864, pp. 1-31. DOI: 10.3390/electronics9111864.

16. Sugiantoro, B., Anshari, M., & Sudrajat, D. Developing framework for web based e-commerce: secure-SDLC. *Journal of Physics: Conference Series*, 2020, vol. 1566, no. 1, article no. 012020, pp. 1-9. DOI: 10.1088/1742-6596/1566/1/012020.

17. Tetskyi, A., Kharchenko, V., Uzun, D., & Nechausov, A. Architecture and Model of Neural Network Based Service for Choice of the Penetration Testing Tools. *International Journal of Computing*, 2021, vol. 20, no. 4, pp. 513-518. DOI: 10.47839/ijc.20.4.2438.

18. Tetskyi, A., Perepelitsyn, A., Illiashenko, O., Morozova, O., & Uzun, D. Ensuring cybersecurity of FPGA as a service with the use of penetration testing of components. *Radioelectronic and Computer Systems*, 2024, no. 2, pp. 160-172. DOI: 10.32620/reks. 2024.2.13.

19. Perepelitsyn, A., & Kulanov, V. Analysis of Ways of Digital Rights Management for FPGA-as-a-Service for AI-Based Solutions. *Proceedings 2023 IEEE 13th International Conference on Dependable Systems, Services and Technologies*, DESSERT 2023, 2023. pp. 1-5, DOI: 10.1109/DESSERT61349. 2023.10416526.

20. *A guide to the PCI DSS compliance levels.* Available: https://www.itgovernance.eu/blog/en/a-guide-to-the-4-pci-dss-compliance-levels (accessed June 7, 2024).

21. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, 2021, vol. 21, no. 14, article no. 4759, pp. 1-28. DOI: 10.3390/s21144759.

22. Owen, H., Zarrin, J., & Pour, S. M. A survey on botnets, issues, threats, methods, detection and prevention. *Journal of Cybersecurity and Privacy*, 2022, vol. 2, no. 1, pp. 74-88. DOI: 10.3390/jcp2010006.

23. Rao, S., Verma, A. K., & Bhatia, T. A review on social spam detection: Challenges, open issues, and future directions. *Expert Systems with Applications*, 2021, no. 186, article no. 115742, pp. 1-31. DOI: 10.1016/j.eswa.2021.115742.

24. Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. Privacy-aware detection framework to mitigate new-age phishing attacks. *Computers & Electrical Engineering*, 2021, vol. 96, article no. 107546, pp. 1-10. DOI: 10.1016/j.compeleceng. 2021.107546.

25. Mahboub, S. A., Ahmed, E. S. A., & Saeed, R. A. Smart IDS and IPS for cyber-physical systems. *Artificial intelligence paradigms for smart cyber-physical systems*, IGI global, 2021, pp. 109-136. DOI: 10.4018/978-1-7998-5101-1.ch006.

26. Sharma, D. S. *Enhancing False Positive Detection in IDS/IPS Using Honeypots: A Case Study with CSE-CIC-2018 Dataset*. Available: https://cdn.iiit.ac.in/cdn/web2py.iiit.ac.in/research_centres/publications/download/masterstthesis.pdf.855db95538568de8.494949545f4879646572616261645f4d535f5068445f5468657369732028332e706466.pdf (accessed June 7, 2024).

27. Hindy, H., Brosset, D., Bayne, E., Seeam, A. K., Tachtatzis, C., Atkinson, R., & Bellekens, X. A taxonomy of network threats and the effect of current datasets on intrusion detection systems. *IEEE Access*, 2020, vol. 8, pp. 104650-104675. DOI: 10.1109/ACCESS.2020.3000179.

28. Kim, A., Park, M., & Lee, D. H. AI-IDS: Application of deep learning to real-time Web intrusion detection. *IEEE Access*, 2020, vol. 8, pp. 70245-70261. DOI: 10.1109/ACCESS.2020.2986882.

29. Ghazi, D. S., Hamid, H. S., Zaiter, M. J., & Behadili, A. S. G. Snort Versus Suricata in Intrusion Detection. *Iraqi Journal of Information and Communication Technology*, 2024, vol. 7, no. 2, pp. 73-88. DOI: 10.31987/ijict.7.2.290.

Received 25.06.2024, Accepted 20.08.2024

СИСТЕМИ ВИЯВЛЕННЯ І ЗАПОБІГАННЯ ВТОРГНЕННЯМ ЯК КОМПОНЕНТ ЗАБЕЗПЕЧЕННЯ ВІДПОВІДНОСТІ НОРМАТИВНИМ ДОКУМЕНТАМ

А. Г. Тецький, Д. Д. Узун

Багато фінансових установ і постачальників платіжних рішень зобов'язані відповідати PCI DSS (Payment Card Industry Data Security Standard). Такі вимоги зрозумілі, оскільки дотримання нормативних вимог допомагає знизити ризики витоку даних і фінансових втрат, пов'язаних із несанкціонованим доступом

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

до даних карток. Наявність підтвердження відповідності PCI DSS свідчить про те, що організація вжила всіх необхідних заходів для захисту даних. Розглянуто приклад вебресурсу, який повинен відповідати нормам PCI DSS. Впровадження та перевірка засобів контролю (заходів) захисту є невід'ємною частиною процесу підтвердження відповідності. Методи, які використовуються в системах виявлення та запобігання вторгненням, мають певні особливості, які перешкоджають широкому та ефективному впровадженню таких систем захисту. **Предметом дослідження** в даній статті є системи виявлення та запобігання вторгненням, які є частиною системи безпеки вебзастосунків. **Метою роботи** є дослідження особливостей методів виявлення та запобігання вторгненням та надання рекомендацій щодо сумісного використання вищевказаних методів. Для досягнення мети вирішуються наступні **завдання**: виявити ієрархію/зв'язок існуючих нормативних документів, згідно яких може проводитися підтвердження відповідності; описати основні положення сертифікації PCI DSS; визначити системи захисту, які можна реалізувати для захисту вебресурсу від кібератак; проаналізувати переваги та недоліки методів, які використовуються в системах виявлення та запобігання вторгненням; надати пропозиції щодо покращення використання систем виявлення та запобігання вторгненням. Виходячи з поставлених завдань, було отримано наступні **результати**. Виявлено, що основною проблемою сигнатурного методу виявлення вторгнень є недостатньо швидке оновлення баз даних сигнатур і можливість модифікації відомих атак таким чином, щоб відомі сигнатури не використовувалися під час атаки. Метод виявлення аномалій характеризується великою кількістю хибних спрацьовувань на початкових етапах впровадження, в цьому випадку необхідно виконати досить ретельне налаштування та навчання системи на основі умовно безпечних дій користувача. **Заключення**. Комбіноване використання методів виявлення атак дає змогу зменшити кількість помилок першого та другого роду, що свідчить про ефективне використання засобів захисту. Вебресурси з такими засобами захисту можуть бути сертифіковані за виконання інших умов нормативного документа.

Ключові слова: кібербезпека; системи захисту; виявлення вторгнень; запобігання вторгнень; верифікація відповідності; нормативні документи; безпека вебзастосунків.

Тецький Артем Григорович – канд. техн. наук, доц. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Узун Дмитро Дмитрович – канд. техн. наук, доц., доц. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Artem Tetskyi – PhD, Associate Professor at the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine,
e-mail: a.tetskiy@csn.khai.edu, ORCID: 0000-0003-1745-2452, Scopus Author ID: 57202894656.

Dmytro Uzun – PhD, Associate Professor, Associate Professor at the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine,
e-mail: d.uzun@csn.khai.edu, ORCID Author ID: 0000-0001-5574-550X, Scopus Author ID: 57194773530.