British Journal of Global Ecology and Sustainable Development
Volume-32, September- 2024
ISSN (E): 2754-9291

DEVELOPMENT OF INFORMATION PROTECTION MODEL IN ".UZ" DOMAIN

Gafurov Sh. A.
Independent Researcher of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract:
In this article protection of information systems in domains located in the uz domain of the national segment of the Internet network and its levels, the processes of organizing a complex protection system, the tasks of each level, and a model of protection of information systems are proposed.

Keywords: malicious traffic, IDS/IPS, eGov system, cyber-attacks, web resources, national segment, threat.

Introduction

Today to ensure the security of the ".uz" domain shows that the development of new types of protection mechanisms and their implementation by state and non-state organizations by companies developing protection tools the number of requirements for the provided services has increased dramatically, and every organization has been carrying out the necessary organizational technical work for the protection of the official web page and the web platforms developed for providing interactive services. Web pages located in the national segment section of each country may not belong to organizations or businesses located in that particular country. The main reason for this is that when purchasing a domain for their web pages, organizations can make a voluntary choice depending on the quality of service provided by domain providers (the web pages of government organizations must be in the national segment) .

Most of the threats to web pages located in the national segment are aimed at the web resource platform. The main reason for this is that if a vulnerability is detected in a specific website, the attacker can almost only get the data of that website, but if any vulnerability is detected in the domain platform where the website is located, then he can get the data of all the websites in the domain platform. can be Therefore, as the number of network attacks directed at web pages and web resources increases, so does the demand for network intrusion detection and prevention systems (IDP/IPS) for information security. Typically, attack detection and mitigation systems are considered to have different architectures. It is necessary to pay special attention to the classification of IDS/IPS systems, because experts make decisions about which software product to use in this or that situation using the generally accepted IDS classification. Network differentiation of IDS/IPS systems is currently the most popular method. In addition, there are other schemes of classification of the protection system of different levels of detail and marked information. Existing systems perform the following additional tasks in addition to their main functions.

Journal Zone Publishing, Ilford, United Kingdom

- notify employees of known attacks detected;
- study obscure sources of information about attacks;
- reducing the load of requests to the administrator responding to security from daily operations on the control of users, information systems and networks, which are components of the corporate network;
- to enable users who are not experts in the field of information security to manage protection tools.

Based on these, it is proposed to implement the protection model of information systems in the national segment of the Internet network as follows. The main goal is to increase the reliability and efficiency of the protection mechanism. The model is based on nine protection and five analysis principles.

The proposed protection mechanism based on nine protection and five analysis principles, in addition to protection against threats and network attacks to websites located in the national segment of the Internet network, allows to build a comprehensive protection mechanism of protection software tools developed on the basis of modern technologies to ensure the safety of network users. gives

nine protection and five analysis, the proposed protection mechanism includes 9 protection levels and 5 analysis levels, and the Internet network is protected from cyber threats in various forms of cyber management system of multi-layer security. ensures the safety of the national segment. This, in turn, allows to ensure the security of interactive services of the electronic government system.

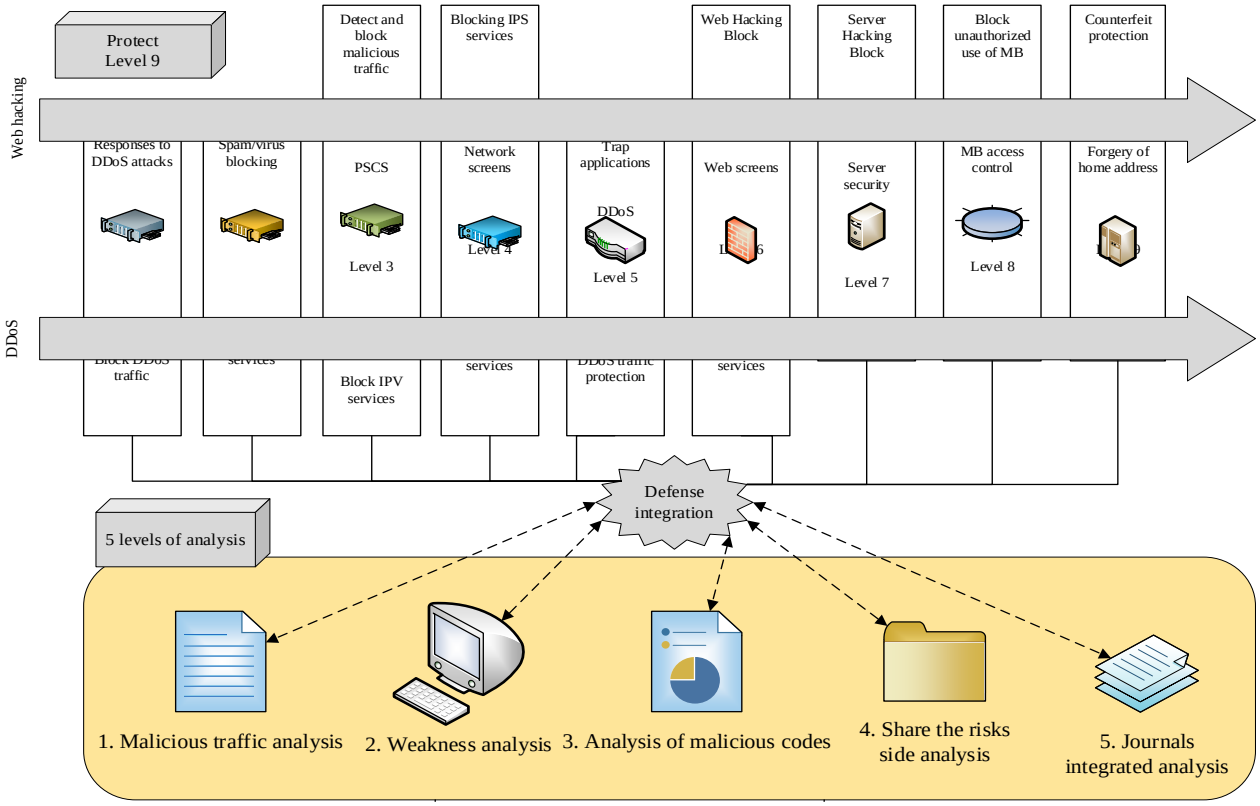

Figure 1. Protection model of information systems in the ".uz" domain of the Internet network

Journal Zone Publishing, Ilford, United Kingdom

Protection levels in the protection model of information systems in the ".uz" domain of the Internet network, in turn, perform the following main tasks.

Level 1 protection serves to prevent DDos attacks by blocking DDos traffic. The system provides network traffic monitoring, anomaly detection, and attack protection from the network layer to the application layer of the TCP/IP protocol stack without affecting the underlying allowed traffic. The main organizational elements of information security (according to the concept of information security) are confidentiality, integrity and usability. A denial of service (DoS) attack affects the availability of information resources. A denial of service is considered successful if it disrupts the availability of the information resource. The success of an executed attack varies by the degree of impact and damage it causes to the targeted web resources. For example, if an online store located in the national segment is attacked, then the long-term interruption of service will obviously cause economic damage to the company. In this case, the attack may cause direct damage, or create a threat and potential risk of damage. However, an attack can be made at any level. In practice, attacks are mostly carried out at layers 3-4 and 7 of the OSI model.

2nd level of protection designed to block spam messages and viruses. Real-time detection of spam and elimination of leakage of corporate information, as well as protection against phishing, viruses, spam, allows protecting corporate mail from global threats, and serves as a protection mechanism that identifies and monitors attacks in the global network.

3rd level of protection designed to detect and block malicious traffic. The key feature is application control and zero-day vulnerability detection. In addition, this level is a level that allows checking the possibility of web application ranking, filtering web application URLs, and ensuring the security of information systems and user traffic.

4th level of protection It is done using an inter-network screen. This is done by blocking unauthorized situations and without any impact on the traffic of network users, for this the following methods are used. These are:

- lists (white, black, gray);
- ru xsat;
- change traffic routes;
- apply traffic filters.

5th level of protection is the level of protection against attacks such as masking using programs that send personal information on corporate networks. The main purpose of such protection is to monitor intruders in the current time interval or to detect attacks carried out by them on corporate networks. From time to time, fake logins and passwords are provided by the program to simulate a data leak. In addition, fake systems

Journal Zone Publishing, Ilford, United Kingdom

that simulate real human communication (the process of information exchange in the network) can be used to confuse attackers. Experts call such sessions "bait sessions".

6th level of protection provides a protection mechanism based on the additional functions of the fourth-level firewall, i.e., the web firewall service is activated. This protection blocks unauthorized web services.

7th level of protection is to ensure server security. At this level, there are three levels of security for the server:
1. Minimum level of security.
2. Resistance to hacking.
3. Detect attacks and weaken their impact.
The level of security of the software can be assessed first by analyzing the attacks that have been carried out against servers with the same software installed. The number of attacks shows how well the software tolerates it. In addition, software reliability directly depends on its quality. Low-quality software does not take into account all the requirements for a security system and is therefore considered an unreliable tool.

Him oya's 8th level. Database access control. Issues to be resolved in the database protection system:
- to determine the presence of restricted information based on remote scanning of database contents.
- quick detection of attempts to use information in the database without authorization and taking measures.
- quick monitoring of the state of database security for company management.

9th level of protection is to protect the home page from spoofing. It is understandable that the number of fraudsters increases proportionally with the increase in Internet activity and the number of users on the world wide web. The most common scams on the Internet are stealing money using fake sites. An unskilled user sometimes has a high chance of connecting to a fake site because he cannot choose the real site from among the many. Fake sites of social networks, banks and financial organizations are especially dangerous. Many bank auction, public file exchange systems and fake sites on social networks have been identified. The last level of protection allows you to protect against such situations.
Based on the taxonomy of possible threats to information resources located in the “.uz” domain of the Internet network, it can be said that the analysis of existing approaches is not always accurate and reliable. This is due to the incompleteness of the analysis data. In some cases, it will be possible to combine several approaches conducted on different characteristic parameters with the help of a single classification. It follows from this that expanding the field of studying potential threats and ensuring the protection of web applications and resources located in the “.uz” domain of the Internet requires

Journal Zone Publishing, Ilford, United Kingdom

improvement of models, methods and algorithms, as well as offering new protection mechanisms.

The main focus in identifying threats and attacks on web applications and resources located in the ".uz" domain of the Internet network is to determine the probability that an attacker will gain access to his target object by successfully violating the current security policy. In addition, it is desirable to determine the exact category of attack, because there are so many types of network attacks in the national segment that it is impossible to create a protection mechanism for each of them. The solution is to categorize network attacks and group them according to attack type. The defense mechanism is formed specifically for attack groups.

References

1 CM Ahmed, MR Gauthama Raman, and A. P. Mathur, "Challenges in Machine Learning based approaches for Real-Time Anomaly Detection in Industrial Control Systems," CPSS 2020 - Proc. 6th ACM Cyber-Physical Syst. Secure. Work. Co-located with AsiaCCS 2020, pp. 23–29 .

2 B.A. A. Al'Aziz, P. Sukarno, and A. A. Wardana, "Blacklisted IP distribution system to handle DDoS attacks on IPS Snort based on Blockchain," Proceeding - 6th Inf. Technol. Int. Semin. ITIS 2020, pp. 41–45

3 V. Hajisalem, S. Babaie, A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection, Comput. Netw. 136 (2018) 37–50,

4 M.A. Ferrag, L. Maglaras, S. Moschoyiannis, H . Janicke, Deep learning for cyber security intrusion detection: approaches, datasets, and comparative studies, J. Inf. Secure. Appl. (2020) 50, https://d o i. org /10.1016/ j.jis a.2019.102419 .

5 I. Sharafaldin, A.H. Lashkari, A.A. Ghorbani, Toward generating a new intrusion detection dataset and intrusion traffic characterization, in: ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secure. Priv., 2018, pp. 108–116.

Journal Zone Publishing, Ilford, United Kingdom