INFORMATION SECURITY MONITORING IN THE ELECTRONIC GOVERNMENT SYSTEM

Gafurov Sh. R.
Independent researcher of TUIT named after Muhammad al-Khwarizmi

Abstract:
To identify incorrect or suspicious actions and operations in voluntary web applications connected to the e-government system, it is necessary to have documented and regulated standards for monitoring and analyzing log entries, network activities and operations. This article discusses the use of information security in the e-government system to detect illegal actions monitoring is proposed.

Keywords: e-government, backup, monitoring, information security, random threats, incidents.

Information security monitoring in the e-government system is the process of continuous monitoring of objects and entities that affect the information security of information and telecommunication networks, as well as the collection, analysis and synthesis of monitoring results. In such cases, it is recommended to use information security monitoring systems using special software or hardware tools to analyze logging data, actions, and operations.

The information security monitoring system is a centralized component designed to automate the process of analyzing information security-related messages from information security tools and increase the efficiency of managing the information and telecommunications network infrastructure in general. Depending on the number of web applications connected to the e-government system and the interactive services provided through these applications, the information security monitoring system can be a specialized software tool or a whole set of software and hardware tools[1].

The development of the first software for information security monitoring systems for the entire corporate network spanned 2000-2002, but the development of digital technologies has led to the development of such software tools, which has led to the improvement and expansion of this type of software . For example, when monitoring systems were first developed, they only allowed for monitoring activity in the system, but today they have advanced to the point where they can provide real-time event reporting, block undetected events, and analyze new types of events and predict future events based on artificial intelligence algorithms. In addition, the information security monitoring systems used today allow for real-time monitoring of not only the behavior of organization employees in the system, but also the national segment environment, user environment, and server environment, which are integrated with the

information systems of corporations and websites of all government agencies at the government level. The main goal of using information security monitoring in the e-government system is to increase the security level of information and telecommunications resources and, as a result, to collect, combine, correlate, and visualize large amounts of information security monitoring data obtained from information security systems, along with controlling the operation of information security systems [2, pp. 1838-1855].

The software or hardware used to implement information security monitoring in the e-government system is required to be integrated with the following software tools, since such software tools can perform the functions of any module of the monitoring system:

- Access control tools are authentication, authorization, and logging servers. Each time a user attempts to log in to an electronic resource, the web application requests confirmation from the authentication server, which checks the security policy and rules before responding. The successful or unsuccessful login results are recorded in the logging server;
- Network firewalls are software or hardware tools that implement access control policies between two networks based on various traffic filtering rules;
- Intrusion detection and prevention systems, or intrusion detection and prevention systems (IDS/IPS), are tools that monitor network traffic and detect signs of traffic scanning attempts, denial of service attacks, or other attacks;
- Host-level IDS are software tools that monitor system or application logs. If a user performs unauthorized actions, that is, attempts to use data, files, or services without permission, these tools give a signal and begin taking protective measures;
- Host-level IPS - detects network usage and anomalies associated with this type of attack. Once an anomaly is detected, the protection system determines whether this anomaly is real or indicates an attack;
- Content filtering and web application protection tools are tools that protect web applications and their resources or organizational assets from threats such as theft, forgery of sales transactions, obtaining personal information about customers, and swapping pages on a website;
- Anti-spam tools are software protection tools for mail servers or gateways. They receive and filter incoming mail, including attachments, based on criteria specified by the server or in the end user's mailboxes;
- antivirus software - software for detecting computer viruses (antiviruses);
- Data leakage protection tools are software tools that enable the detection of unauthorized data leakage and the protection of confidential and personal information from being distributed outside the organization (DLP)[3].

The process of monitoring information security in the e-government system is implemented in four stages.

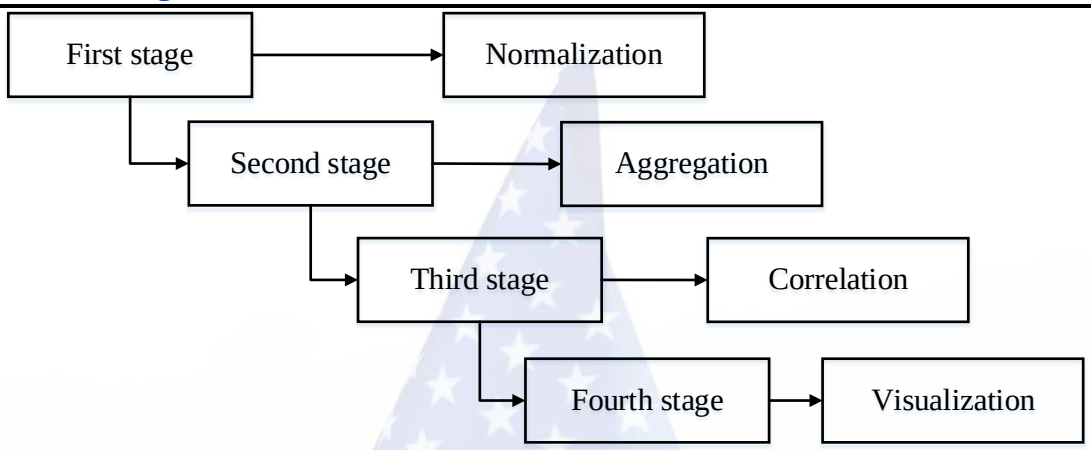

Figure 1. The process of information security monitoring in the e-government system.

Normalization is the process of collecting various messages about events from monitored objects and bringing them into a single format.

Aggregation - a systematic assessment of events that allows you to identify and remove duplicate messages, classify the remaining messages into different categories, identify all events that affect information security, and prioritize information security events;

Correlation – analyzing collected data and identifying signs that indicate an attack;

Visualization is a graphical representation of information security incidents that have passed all previous stages, allowing qualified personnel to identify attacks and take appropriate measures to prevent them in the future and eliminate the consequences of attacks that have already occurred [4].

Based on the above information, the introduction of an information security monitoring system to ensure information security in the e-government system will create the opportunity to solve the following tasks with the help of software tools that require integration into the system:

- real-time monitoring of events on all web resources integrated into the e-government system and located in the national segment environment;
- Dynamic visualization of attacks on a single management console to analyze and make decisions based on the collected data and predict the final outcome of subsequent events;
- information security event logs (log files);
- Respond promptly to potential threats to information security and quickly resolve problematic security situations;
- Creating graphical reports on information security incidents.

If these tasks are implemented in a timely manner, the scope of tasks will expand and the following additional opportunities will be created:

- Assess the risk of information security breaches to analyze the overall security of the network environment in which the e-government system is located and the assets located in this network;

- to document information security incidents (a collection of all actions taken by the system) in a specified file type (.doc, .docx, .pdf, etc.) and maintain a database of the electronic government system for processing information security incidents;
- long-term storage of information from the information security monitoring system (data backup) to provide the necessary information through the system during inspections and monitor the information security status of the e-government system over time [5, pp. 154-158].

Conclusion

To implement information security monitoring in the e-government system and monitor all events on web portals located in the national segment environment and providing state interactive services, and to warn system administrators in case of unauthorized events and temporarily block the operation mode of any module of the system until this situation is eliminated. It allows you to visualize the dynamics of events in an easy-to-understand format for the system administrator by generating reports on situations.

References:

1. L. Dewei, S. Haosong, L. Chenhan, D. Ning, W. Binxin and L. Jinhu, "New Energy Operation Platform Monitoring Data Verification Method Based on Correlation Analysis Algorithm," 2022 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), Dalian, China, 2022, pp. 593-597.
2. J. Zhao, R. Masood and S. Seneviratne, "A Review of Computer Vision Methods in Network Security," in IEEE Communications Surveys & Tutorials, 2021 vol. 23, no. 3, pp. 1838-1878.
3. Botirov Fayzullajon,Yusupov Bakhadir, Gafurov Sharifjon, Assessment of reliability of information protection means in information security monitoring systems. Havo hujumidan mudofaa tizimidagi mutaxassislarni 199 tayyorlashda axborot – kommunikatsiya texnologiyalaridan foydalanish Xalqaro onlayn ilmiy –amaliy konfrensiya, Toshkent 2021, p. 381-387
4. H. Huawei, S. Ning, X. Wei, W. Chunli and J. Weiwei, "Alarm Root-Cause Identification for Petrochemical Process System Based on Fluctuation Correlation Analysis," 2019 Chinese Control And Decision Conference (CCDC), Nanchang, China, 2019, pp. 373-376.
5. X. Duan, Y. Zhou and J. Guan, "Exploration on Heterogeneous Network Security Monitoring Algorithm Based on Big data Intelligent Information Technology," 2023 IEEE 15th International Conference on Computational Intelligence and Communication Networks (CICN), Bangkok, Thailand, 2023, pp. 154-158.