ATLANTIS PRESS

Advances in Computer Science Research, volume 65

3rd International Conference on Communications, Information Management and Network Security (CIMNS 2018)

Methods of Testing of the Corporate Network's Traffic Anomalies

Nikita Kulyasov and Sergey Isaev

Institute of Computational Modelling of the Siberian Branch of the Russian Academy of Sciences, Akademgorodok 50/44, 660036 Krasnoyarsk, Russia

***Abstract*—This article gives an overview of the existing methods and software products designed to analyze anomalies that may indicate the occurrence of cyber-threats. On their basis, we propose our own original software tool that allows automatic detection of anomalies and subsequent detailed analysis of network service logs according to the metrics chosen by the administrator. The software tool is designed as a web application integrated into the existing infrastructure of the corporate network of a scientific organization. Implementation of our web application showed the relevance and demand of the anomaly detection systems' development.**

Keywords—network anomalies; cybersecurity; anomaly detection system; intrusion detection system

I. INTRODUCTION

Development of modern information technologies lead to higher informatization and transfer of scientific and production processes to the cyberspace. Global computer networks are deeply integrated in companies' operation. Quick access to information helps to decrease production cost, increases efficiency and profitability of the companies. On the other hand, such integration may lead to problems and loss of data's confidentiality in case of unauthorized intrusions. It burdens corporate security systems.

In this article we suggest the methods for detection of network threats and describe software designed to prevent threats and protect the corporate network of a scientific center [1]. Our work is based on analysis of the anomalies of network traffic. Anomaly is something that is different from normal. We understand network anomalies as abnormal use of network resources accessed via WEB-services and network applications.

Anomaly detection nowadays is one of the actively developing area of the cybersecurity. It's because anomalies in most of the cases are the beginning of network attacks that may cause non-material and financial losses for the companies that are substantially presented in the cyberspace. As a rule, such anomalies are the results of spying or "power trial" for further use of the revealed problems in the security system in order to get commercial profit. Detection and classifying of anomalies implies continuous monitoring of the events in the computer systems and networks, and requires processing of the large data volumes generated by these sources. For these purposes, automated attack detection systems are used [2]. There are commercial software tools allowing to analyze traffic with regard to anomalies and threats in real time. Usage of these systems are limited by high cost and closed architecture and it's difficult to adjust them to a company's infrastructure.

Many modern scientific studies are dedicated to the methods of analysis of network traffic's anomalies. They describe modern types of the detection systems and different techniques of network attack detection and promising directions of their development [3]. Disadvantages of the existing systems are high level of false alarms and difficulty to create training set. Usage of the generalized classification [4] allows to partially redress the first disadvantage, providing a transparent set of features for anomaly identification. For accurate anomaly detection, different algorithms are used. For example, the method of cascade clastering in combination with the decision trees [5] allows to achieve high accuracy of the test data and the level of anomaly detection over 90%. Hybrid methods of anomaly detection based on neuro fuzzy and immune classificators [6] allow to reach a compromise between the accuracy of anomaly detection and search of the unknown types of threats. Methods of multi-factor analysis for CPU utilization time series [7] didn't show high results and they require precise selection of parameters for analysis. In this work [8] we applied the methods of clastering using assessment of density in the event characteristics' space. Most of the studies that we reviewed are theoretical and very hard for implementation with regard to the suggested methods and algorithms, so in practice they don't provide an easy solution of tasks of information security.

For network threats detection, we've created software tool "Network service log's automated analysis system" integrated in the existing infrastructure of a scientific center's corporate network providing function with minimum resources. This new software expands the existing means of security by additional services designed to reveal anomalies at the boundary sections of the corporate network's infrastructure. Usage of the "Network service log's automated analysis system" allows to configure the first line of network attack security due to indication of the incidents overlooked by the standard protection means. It also ensures higher security of network resources and quick response.

II. TASKS OF THE "NETWORK SERVICE LOG'S AUTOMATED ANALYSIS SYSTEM"

The basis of creation of an automated system for network service log's analysis is the model of a scientific center's information security (Fig.1).

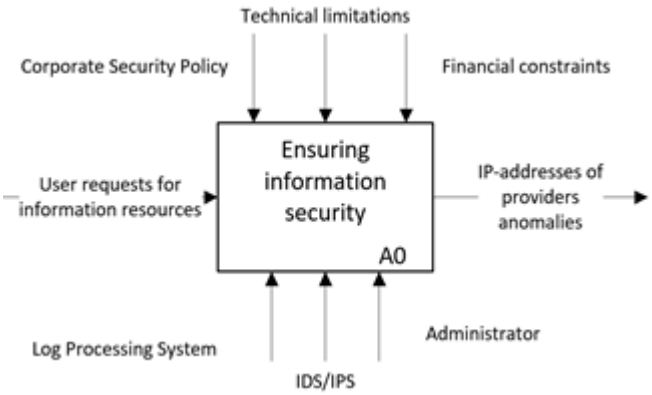

FIGURE I. SCIENTIFIC CENTER'S INFORMATION SECURITY MODEL

Information security requires consideration of the restrictions based on the security policy of an organization [10], its technical equipment and financial limits. Input parameter of this model is interaction of a user with the network services of an organization documented in log-files. The executors are: service administrators, the already integrated systems of attack detection/prevention and the proposed system of network service log's processing. As a result, we have a list of IP-addresses of the sources of anomalies and potential security threats.

Thus, the key tasks of the log analysis automated system are:

1. Automation of the processes of network service log's analysis.

2. Aggregation of data of several network services.

3. Creation of an interactive interface to demonstrate data and results of the analysis.

Solution of these tasks allows building of a system similar to attack detection nodal systems with regard to their functionality [12]. In order to detect and analyze threats, the logs of network services: web-server, ftp-server and firewall are reviewed.

We suggest the following function model of the anomaly detection automated system (Fig.2).

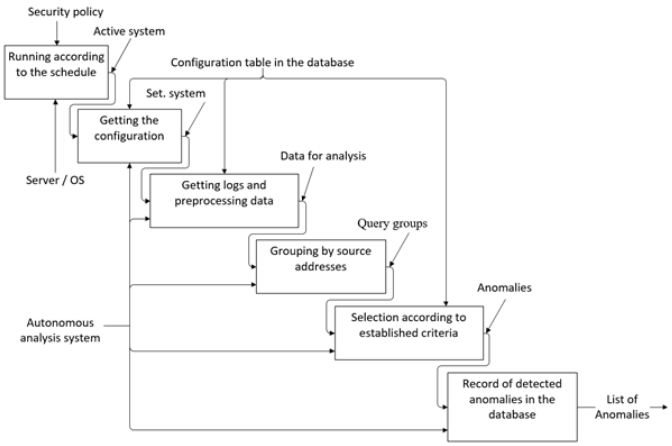

FIGURE II. SYSTEM'S FUNCTIONAL MODEL

The model describes functional blocks responsible for: automation; reception of the analysis system's configuration from DBMS; data reception, pre-processing and analysis; recording of the detected anomalies in the DBMS table.

The model supports cross-platform implementation of software for its further usage under control of the operating systems Windows and Unix. System's data storage is completed in the cross-platform DBMS MySQL. Task management utility "cron" for Unix and "Task Planner for Windows" are used for automation purposes. These planners are integrated in most of the operating systems' distributives. They provide flexible setup of application launch timetable, minimization of user's participation in the process of program execution after it's set up and in this way, provide the required automation of data processing. The configuration table of the data base contains the parameters of system's function: "IP address of node under study", "service's name", "records for service log's acquisition", "log layout in the file system", "names of web-service's log's", "names of ftp-service's logs, "name of firewall's log", "type of the applied software", "parameters of anomalies typical for a given service", "list of the acceptable addresses determined by administrator".

After launch, application requests the base for the sources and then receives ftp logs. Each log is analyzed by program one by one in a background mode. Simultaneously, data is processed, so the processes of analysis and function of the system in whole go quicker.

In order to group data on the set criteria, it is filtered in accordance with the IP-addresses of the local services of organization that are a part of the list of the acceptable addresses determined by administrator. After filtering, only the records of the time period that must be analyzed, are left in the local copy of the log file. At the next stage, the records are grouped in accordance with the source's address and are checked with the anomaly metrics set in the configuration. If a group of inquiries satisfies or exceeds the set values, its source is marked as the source of anomaly and an appropriate record is entered in the table of anomalies. The results of the anomaly analysis are displayed in the software's interface.

These processes allow to aggregate data of several network services.

III. Implementation Of The "Network Service Log's Automated Analysis System"

The software "Network service log's automated analysis system" has a web-interface [13] and can be built in the existing information services of a co rporate network. It is designed with the use of the following software tools: languages HTML, CSS, JS, PHP and libraries for data interaction: Jquery, D3.js, DC.js. In order to provide system's security and support of the collected data, the records are exported to a csv-format file. The software's interface interacts with the data represented in a csv-file.

Visualization of network threats' anomalies is completed in a form of interactive diagrams demonstrating the number of the detected anomalies at a t ime period, threat source location diagrams, histograms, different charts of network threat location. The examples of circle diagrams are presented in Fig.3.

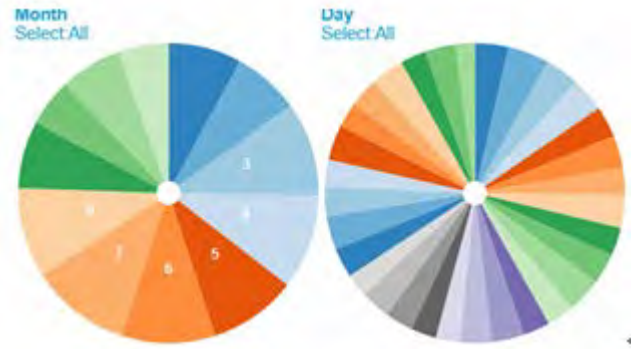

FIGURE III. DIAGRAMS OF THE NUMBER OF DETECTED ANOMALIIES

Histograms displaying the number and type of anomalies are presented in Fig. 4.

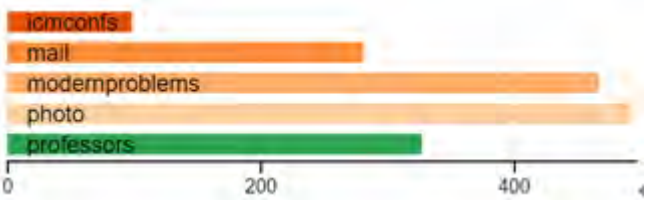

FIGURE IV. HISTOGRAMS OF THE DETECTED ANOMALIES

Software visualizes statistics of the log analysis in a chosen time period. User can change the parameters of presentation by choosing the value for diagram building: the quantity of threshold excess or a total number of appeals during the incident. The statistics on the most active clients (confirmed threats) is displayed in the form of column diagrams.

The program allows to study the diagrams of threat agents' statistics at network interface ports, choose data on specific clients for getting detailed information about the sources of anomalies [14].

An example of the diagram of anomalies' activity distribution by time periods is presented in Fig. 5.

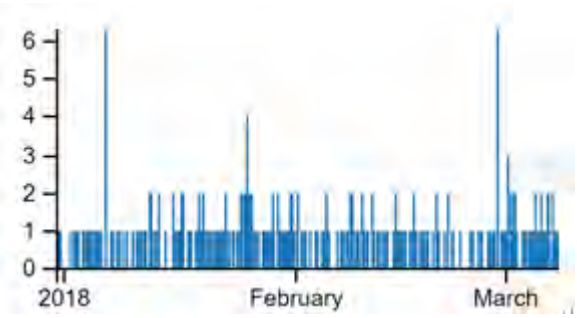

FIGURE V. DIAGRAM OF ANOMALIES' ACTIVITY DISTRIBUTION AT A TIME PERIOD

The most of the analyzed data is contained in firewall logs, so in order to analyze it software provides additional options. The results of the firewall log's analysis are displayed on a separate page of the software's interface that contains detailed statistics and a way to compare several indicators and also the tool for additional statistical researches. For processing large volumes of data, there is a possibility to set a time period for analysis, so this way interface keeps to respond quickly and supports comfortable interaction with the users.

For detection of the possible relationships of the events at different ports of network interfaces, software provides calculation of coefficients of correlation and chart building for the chosen ports (Fig. 6). Event is understood as the number of recorded trials to access a port at a time period or a number of threshold excesses.

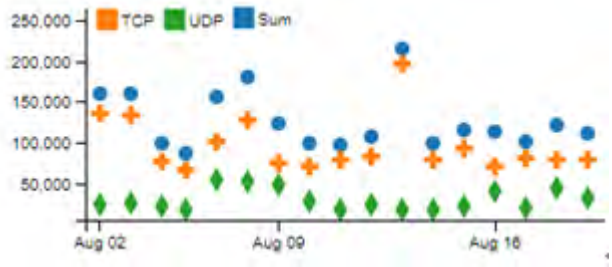

FIGURE VI. DIAGRAMS OF CORRELATION OF THE SERVICES EXPOSED TO ANOMALIES

The information acquired through the system and the conclusions made on t he basis of its further analysis can be used for correction of the active information security systems and for prevention of the incidents characterized by such events in future.

IV. Conclusion

We've studied network anomalies for Internet service logs and suggested a modified model for providing information security of the corporate network. Realization of this model in form of a web-application allowed to conduct an analysis of threats and reveal topicality of development of the anomaly analysis systems and their integration in the infrastructure of an organization.

The result of our work is a fully functional software "Network log's automated analysis system". The system has additional services for corporate network security. They are

designed to detect network anomalies at the boarder sections of an infrastructure.

Our system contains analytical instruments for detection and study of the potentially dangerous network anomalies. It allows to group and aggregate data, build statistical diagrams of threat agents' activity, reveal dependencies between abnormal events and calculate coefficients of linear correlation for specific services. Analytical functions realized in the interactive interface of the software allow to get a clear picture of a studied anomaly in a real-time mode. Components of our software increase the efficiency of use of the standard attack detection and prevention systems due to detection and account of new nonstandard factors and dependencies.

"Network service log's automated analysis system" was tested and implemented in the Krasnoyarsk Science Center's corporate network infrastructure. Its usage allowed to make configuration of the security system's first protection line against network attacks, considering the revealed incidents and sources of threats that earlier were not considered in standard protection means. Thus, quick response to threats and the overall level of cyber-security of the organization have been increased.

REFERENCES

[1] Isaev S.V. Cybersecurity of a scientific institution - assets and threats // Informatizatsiya i svyaz, No. 1, 2015. pp. 53-57.

[2] Papadaki M. F.S.. IDS or IPS: what is best? // Network Security, No. 7, 2004. pp. 15-19.

[3] Zonghua Zhang, Ahmed Meddahi. Security in Network Functions Virtualization // Elsevier, 2012, pp 157-172.

[4] Matthew Roughan, Kenjiro Cho, Paul Tune. A BasisEvolution framework for network traffic anomaly detection // Computer Networks, No. 135, 2018, pp 15-31.

[5] Muniyandi A.P. Network Anomaly Detection by Cascading K-Means Clustering and C4.5 Decision Tree algorithm // Procedia Engineering, No. 30, 2012. pp. 174-182.

[6] Branickij A.A., Kotenko I.V. Detection of network attacks based on the integration of neural, immune and neuron-fuzzy classifiers // Informacionno-upravljajushhie sistemy. 2015. №4 (77).

[7] Basarab M. A, Stroganov I. S. Detection of anomalies in information processes based on multifractal analysis // Voprosy kiberbezopasnosti. 2014. №4 (7).

[8] Nesterenko V. A. Construction and use of the density function in the characteristic space to detect abnormal events // Izvestija JuFU. Tehnicheskie nauki. 2008. №8.

[9] Xavier Clotet, José Moyano, Gladys León. A real-time anomaly-based IDS for cyber-attack detection at the industrial process level of Critical Infrastructures // International Journal of Critical Infrastructure Protection. 2018.

[10] Kononov D., Isaev S. Improving Web Applications Security Using Path-Based Role Access Control Model // 2018 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC), 2018, pp 1-4, doi: 10.1109/RPC.2018.8482195.

[11] Ma xiaojuan. Research and Implementation of Computer Data Security Management System // Procedia Engineering. 2017. №174. Pp 1371-1379.

[12] Babenko G.V. Analysis of current threats to information security arising from network interaction // Vestnik AGTU. Seriya: Upravlenie, vyichislitelnaya tehnika i informatika, No. 2, 2010.

[13] Shepelev A.N., Bukatov A.A., Pyihalov A.V. Analysis of approaches and tools for processing service logs // IVD, No. 4(27), 2013.

Ivanov A.N., Koznov D.V., Tyijgeev M.G. Modeling the interface of full-featured Web-based applications that work intensively with data // Vestnik SPbGU. Seriya 10. Prikladnaya matematika. Informatika. Protsessyi upravleniya, No. 3, 2009