A Data Collection and Analysis System for Managing the Vulnerabilities of Users of an Information System in a Small Business

Liudmila Astakhova
Information Security Department
South Ural State University
Chelyabinsk, Russia,
professor
astakhovalv@susu.ru

Nikita Muravyov,
Information Security Department,
South Ural State University,
Chelyabinsk, Russia,
student
mns7496@yandex.ru

***Abstract* – The relevance of the article is due to consistently high indicators of the number of information security (IS) incidents caused by users of the corporate network and limited financial resources to protect information in small enterprises. Revealed a great interest in theoretical and practical issues of proactive protection of information systems and behavioral analysis - User and Entity Behavi[1]oral Analytics (UEBA) to solve the problems of personnel security of information systems. However, despite the intensive development of the UEBA solutions market, they do not sufficiently reflect the context of user behavior and are not used in small enterprises due to resource constraints. To solve these problems, the authors of the article have developed an information and analytical system for the Vulnerability Assessment of Information System Users (EVISU) for a small enterprise. The approach to solving this problem based on the integration of UEBA, Behavioral Biometrics (BB) and Open Source Intelligence (OSINT) technologies is substantiated. The functional novelty of the system is the extension of the monitoring object due to the context of user behavior: the possibility of biometric recognition of persons who have legitimate rights to access information; the ability to monitor and evaluate not only internal but also external user behavior. As a tool to determine the level of user vulnerability, a "Safe User Profile" is proposed. The practical result of the work is the successful testing of the IAS EVISU in a small enterprise for the production of software products.**

Keywords - information security, information system, user, behavioral analysis, vulnerability.

I. Introduction

In the first half of 2018, 64.5% of information leaks occurred due to the fault of an internal violator, which is 4 percent more than in the same period of 2017 [1,2]. Therefore, the intensive development of behavioral analysis of users and entities - to solve the problems of proactive information protection in information systems is so timely. The nature of the actions of the intruder can be either intentional or unintentional. So, in 2017, the share of intentional data leakage amounted to 87.2% [2].

The work was supported by Act 211 Government of the Russian Federation, contract № 02. A03.21.0011

However, this important context of the actions of the violator of the rules of information security in UEBA-technologies is not implemented, which complicates the decision-making process, especially in small organizations with limited resources. This is the purpose of the article - to develop the concept of a system of information-analytical system for assessing the vulnerabilities of users of an information system, taking into account the contexts of their behavior, implement this concept in a software-technical solution based on modern technologies and test it in practice.

II. Literature Review

According to the well-known American research and consulting company Gartner, which specializes in information technology markets, behavioral analysis is one of ten strategic technology trends in 2018. UBA or UEBA is a cybersecurity process for detecting internal threats, targeted attacks, and financial fraud. UEBA solutions consider models of human behavior, and then use algorithms and statistical analysis to identify significant anomalies of those patterns that indicate potential threats [3,4]. UEBA modules already track user behavior, as well as information about IP addresses and devices in enterprises [5].

Behavioral approach is used in the study of encroachments on the confidentiality of users of applications. This allows mobile behavioral analytics to be used to collect detailed information on the use of applications and templates [6]. In order to deepen understanding of user behavior, the authors demonstrate the advantages of combining web application models with event logs [7].

The market of behavioral analysis systems - User UBA / UEBA is developing intensively. UEBA systems are presented both as separate software solutions and as extensions for already existing systems: SIEM (Security Information and Event Management), DLP (Data Loss Prevention), EDR (Endpoint Detection and Response), etc. [8].

According to the Gartner forecast, “by 2020, at least 60% of the global cloud backing can be defined as the SIEM and the DLP vendor will incorporate " [9]. Anomalous user behavior in UEBA systems is determined using machine learning mechanisms. A huge role here is played by the number of sources of information on the typical working day of a particular employee and the dynamic adjustment of his profile based on mathematical statistics methods to reduce the percentage of false positives [10].

UEBA frees up human resources to work on creating information security strategies, addressing vulnerabilities, responding to threats, educating people, etc. [11]. However, the deepening of the behavioral analysis of users naturally generates interest in the other side of the problem - the humanitarian: norms and standards in the field of human rights [12]. Scientists are concerned about how to ensure confidentiality and protect personal data of users, when the technology is fully based on constant monitoring of their digital world [13]. Moreover, many active authentication technologies have a vulnerable link - the ability to steal information collected in the process of tracking a user and falsify the algorithms that process it.

BB is used for user profiling today. Unlike the old identification methods, it allows the computer to identify the user by its behavior. The US Agency for Advanced Research DARPA proposed to call this class of innovative approaches to the identification of "Active Authentication" (AA). This set of concepts and models of “behavioral analysis” will allow computers without the use of long and hard-to-remember passwords to independently recognize their users by the types of activity that are strictly individual for the ordinary activities of every single person. Such types of activity include, for example, keyboard handwriting, peculiarities of finger movements when working with a mouse, screen, touch pad and other manipulators. The existing hardware of smartphones and tablets also makes it possible to effectively recognize people by the characteristics of their face, gait or location, the specifics of clothing style or surrounding interiors, the characteristics of breathing and heartbeat. [14].

Existing UEBA solutions, apart from advantages, have disadvantages: they cannot provide enough information about the context: whether there is a production need for access to data, their secrecy, etc. If the identified user actions hypothetically can lead to damage to the organization, then further find out whether this user has legitimate access rights to information, whether his laptop or account [15] was compromised, who, besides the trusted user, was located near his workplace, etc.

We believe that the nature of the user's influence on the information also applies to the contexts of user actions: intentional or unintentional. Reasons for causing a deliberately destabilizing effect include the user's desire: to gain material gain; harm (revenge) the leadership or colleague at work, and sometimes the state; provide disinterested service to a friend from a rival firm; advance in service; to protect oneself, relatives and friends from threats, blackmail, violence; show your importance. [16]. Therefore, it is very important to know the current emotional state of the user and the degree of his vulnerability to prevent information security incidents.

In science and practice, attempts were made to create methodologies for assessing human vulnerabilities of users [17], and also to implement them in software solutions [18]. Different approaches to automating the construction of a user's vulnerability profile were justified by the research team in [19]. The experts also substantiated the variant of the risk behavior model [20]. However, the problems of assessing the context of the behavior of users of the information system are not solved in science and practice.

III. Work Results

To solve the problems of the context, we have developed an information and analytical system for assessing the vulnerabilities of users of the information system based on the integration of modern behavioral analysis technologies, including BB, and OSINT. During the development of software and hardware solutions, we used the technology of machine learning and computer vision.

The system is implemented on a client-server network architecture. The IAS with the developed Web-API technology is deployed on the server side, and an agent program is installed on the user’s side to monitor the actions and send data to the IAS. The functionality of the system includes:

1. Data collection.

1.1 Manual filling out forms for different types of incidents.

1.2 The ability to create your own forms for filling.

1.3 Maintain employee profiles and set up incident-employee communications.

1.4 Automated collection of information about the latest incidents in the field of information security, external monitoring of user activity from open sources on the Internet.

1.5 Automated monitoring of user actions with the help of an agent program that is implemented on the client side and transmits data about actions to the IAS.

2. Analysis of user data.

Functions 1.1 - 1.3 are implemented using a simple database engine for data collection. We have created a data bank consisting of databases of persons, actions, incidents, etc. (Fig. 1). For data storage, there is a system for setting fields: from simple (number, string, date, etc.) to complex, which allow you to establish a connection between the databases (Fig.2, 3).

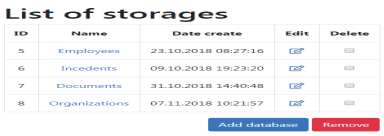

Fig. 1. Sample database list for data storage

Pay attention to the function 1.4. Automated collection of information about the latest information security incidents from open sources on the Internet is due to the need to take into account the context, as we mentioned above. The information community is growing faster and faster, but for operational decision making today is not enough knowledge of the main trends. For example, the first information about malware WannaCry appeared on social networks 6 hours before official publication in the media. If companies knew about it in time, they would have managed to take appropriate measures to protect their systems [21]. Organizations need a quick way to obtain information about current events in the field of information security, so this function will help collect data from popular sources and analyze them according to various criteria.

Fig. 2. Editing Database Fields

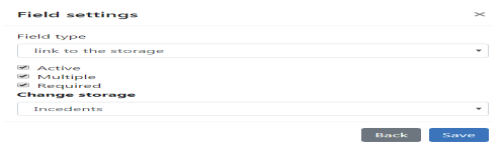

Fig. 3. Setting fields

Recently, there has been a lot of interest in Open Source Intelligence technologies. A company can use OSINT to conduct a risk assessment to identify vulnerabilities before a cyberattack occurs. Using OSINT can increase an organization's awareness of vulnerabilities and, consequently, increase the organization's cybersecurity by identifying actual threats and creating a space for employee training [22]. This technology has allowed us to implement the monitoring of external user actions on open sources on the Internet. In our system, data collection is implemented using the Streaming API on the example of the social network VKontakte. The technology allows you to connect to the data stream in real time and filter it according to specified rules.

It has features and function 1.5 - automated monitoring of user actions within an organization. The program is implemented on the client side and transmits data about actions in the IAS. The solution we developed is able to:

1) monitoring of document printing events (Fig. 4);
2) monitoring file system events (creating, modifying, deleting and copying file system entities (Fig. 5);
3) visual control of unauthorized persons in front of the monitor via a webcam (Fig. 6).

Here are illustrations of the above system functions.

Monitoring document printing events:

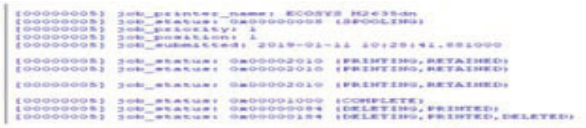

Fig. 4. Example of monitoring print events

Monitoring file system events (creating, modifying, deleting and copying file system objects:

```
2019-03-08 17:07:29 - Created file: .\data.sql
2019-03-08 17:07:29 - Modified file: .\data.sql
2019-03-08 17:07:38 - Deleted file: .\data.sql
```

Fig. 5. Example of tracking the creation, deletion, modification of file system objects

Visual control of outsiders in front of the monitor via a webcam:

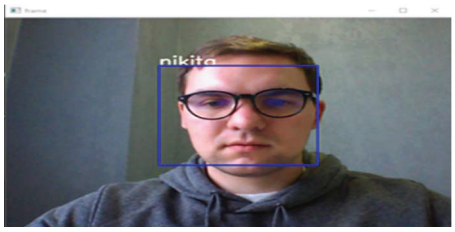

Fig. 6. Face recognition of the current user authorized to the IP.

The face recognition algorithm analyzes the data flow from the camera (Fig. 6). In case of detection of an unrecognized image of a person who is not authorized for this AWS, which may become familiar with restricted access information on the screen, the program takes a snapshot and sends it to the IAS. This function of the IAS allows us to solve another problem of the limited context of user behavior indicated by experts during the analysis of UEBA solutions. To demonstrate the operation, all monitoring data is displayed on the screen, but in real use the program works in hidden mode.

Analysis of user data. As a result of the accumulation of an array of data for a certain period, it becomes possible to use various methods for analyzing them. In our article [23], we illustrated how data are analyzed for several months to predict the growth rate of the threat level in user actions.

To analyze the existing capabilities of the data accumulation platform, according to the criteria of

price / quality / safety / certification, we have selected the 1C-Bitrix framework. To develop a solution on this platform, the most initial version will cost you 5,400 rubles, which is acceptable for small organizations.

The developed system was tested at one of the small enterprises of Chelyabinsk. The results showed that with minimal resource costs, it successfully implements its functionality, and therefore can be used in small organizations in the practice of information protection.

IV. Conclusion

The relevance of recording information about information security incidents due to the user's fault is constantly growing. The article shows the possibilities of a behavioral approach and the disadvantages of UEBA solutions for preventing information security incidents. The scientific novelty consists in the development and program-technical implementation of the concept of an information-analytical system for collecting and analyzing data about users of the corporate network of small enterprises (organizations). The goal of IAS EVISU is to help assess the vulnerabilities of users of an information system in a small organization. The advantages of the developed system are: the accounting of contextual data about the user; resource accessibility for small organizations; ease of integration (no need to have professional knowledge of computer ownership); safe data storage, etc. The practical significance lies in the fact that as a result of testing this system at one of the software production enterprises, the hypothesis was confirmed that operativeness and quality of management decisions in the field of information security would be improved if EVISU IAS was put into practice.

References

[1] Global research on leakage of confidential information in 2017._- URL: https://www.infowatch.ru/report2017. Cited June, 26, 2018.

[2] Global research on confidential information leaks in the first half of 2018. -URL: https://www.infowatch.ru/report2018_half

[3] D.W. Cearley, B. Burke,| S. Searle,| M. J. Walker, “Top 10 Strategic Technology Trends for 2018”. Published: 03 October 2017 ID: G00327329 – URL: https://www.gartner.com/doc/3811368?ref=SiteSearch&sthkw=User%20%20Behavior%20Analytics&fnl=search&srcId=1-3478922254. Cited June, 26, 2018.

[4] A. Litan, M. Nicolett, “Market Guide for User Behavior Analytics. Share this on Facebook Tweet Archived”, Published: 25 August 2014 ID: G00260457 – URL: https://www.gartner.com/doc/2831117/market-guide-user-behavior-analytics. Cited June, 26, 2018.

[5] S. Madhu, S. Min-Yi, W. Jisheng, “User and Entity Behavior Analytics for Enterprise Security”. Proceedings of the 4th IEEE International Conference on Big Data (Big Data) Washington, DC: DEC 05-08, 2016, p.1867-1874.

[6] M. Resnick, A. Leow, J.Wong, “It's Time for App Leadership to Reframe Mobile App Development Decisions”, Share this on Facebook Tweet Published: 28 February 2018 ID: G00323726 – URL: https://www.gartner.com/doc/3863464?ref=SiteSearch&sthkw=User%20%20Behavior%20Analytics&fnl=search&srcId=1-3478922254. Cited June, 26, 2018.

[7] C. Bernaschina, M. Brambilla, A. Mauri, E. Umuhoza, “A Big Data Analysis Framework for Model-Based Web User Behavior Analytics”. In: Cabot J., De Virgilio R., Torlone R. (eds) Web Engineering. ICWE 2017. Lecture Notes in Computer Science, vol. 10360. Springer, Cham

[8] A. Matveev, "Market Overview of Behavioral Analysis Systems - User and Entity Behavioral Analytics (UBA / UEBA)" – URL: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba. Cited June, 26, 2018. (in Russian)

[9] Gartner. "Forecast Snapshot: User and Entity Behavior Analytics", Worldwide, 2017, 03 March 2017, Gartner Event Presentation, To the Point: Understanding the UEBA Landscape, Toby Bussa, Avivah Litan, Gartner Security & Risk Management Summit, 12 –15 June 2017 / National Harbor, MD).

[10] A.S. Artamonov, A.Yu. Ivanov, "Perspective Methods for Analyzing Information Flows in the Sphere of Security of Automated Systems of the Ministry of Emergencies of Russia (Information and Analytical Review - Part 2)", Scientific and Analytical Journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergencies of Russia" 2017, №1. - URL: https://cyberleninka.ru/article/n/perspektivnye-metody-analiza-informatsionnyh-potokov-v-sfere-bezopasnosti-avtomatizirovannyh-sistem-mchs-rossii-informatsionno. Cited June, 26, 2018.

[11] D. Maher, “Can artificial intelligence help in the war on cybercrime?”, Computer Fraud & Security, 2017, Issue 8, pp. 7-9.

[12] A. Liaropoulos, “Cyber-Security: A Human-Centric Approach”, Proceedings of the 14th European conference cyber warfare and security (ECCWS-2015), 2015, pp.: 189-194.

[13] A. Kiss, C. Krasznay, “Cybersecurity Advantages and Privacy Challenges of User Behaviour Analytics”, Informacios tarsadalom, 2017, Vol.17, issue 1, pp: 55- 62.

[14] V.A. Dovgal, D.V. Dovgal, "Analysis of promising methods of behavioral biometrics for user authentication", Bulletin of the Adyghe State University. Series 4: Natural-mathematical and technical sciences, 2017, №3 (206). - URL: https://cyberleninka.ru/article/n/analiz-perspektivnyh-metodov-povedencheskoy-biometrii-dlya-autentifikatsii-polzovateley. Cited April, 09, 2018.

[15] A. Dankevich, "Great expectations: why does UEBA technology not become a silver bullet" - URL: https://www.anti-malware.ru/analytics/Technology_Analysis/why_technology_UEBA_not_be_silver_bullet. Cited June, 26, 2018.

[16] A.I. Aleksentsev, “The Concept and Structure of Threats to Protected Information,” Information Technology Security, 2000, 3, pp.10–17. (in Russian)

[17] L.V. Astakhova, “Human information security vulnerability of organization: methodology of assessment”, Безпека інформації, 2013, Т. 2, № 19, pp. 133-138.

[18] L.V. Astakhova, V.A. Efremov, A.I. Mitkin, "Automation of a Multifactor Assessment of Personnel Vulnerabilities in Information Security", Bulletin of the Urals Federal District. Security in the information sphere, 2014, 4 (14), pp. 57-61.

[19] G.I. Bagretsov, N.A. Shindarev, MV Abramov, T.V. Tulupyeva, "Approaches to the development of models for the analysis of textual information in social network profiles in order to build a profile of user vulnerabilities," International Conference on Soft Computing and Measurements, 2017, T. 1, pp. 134-137.

[20] A.V. Toropova, A.V. Suvorova, T.V. Tulupyeva, "Assessment of data consistency in the risk behavior model", International Conference on Soft Computing and Measurements, 2015, T. 1, pp. 5-8.

[21] D.R. Hayes, F.Cappa, "Open-source intelligence for risk assessment", Business Horizons, 2018, 61 (5) , (September–October 2018), pp.689-697.

[22] IT Information Provisioning System. – URL: https://securitynextgen.ru/pdf/06-PWC.pdf

[23] N.S. Muravyov, L.V. Astakhova, "Prevention of incidents of information security based on user profiling: software and hardware", Bulletin of the Urals Federal District. Security in the information sphere, 2018, 1 (27), pp.66-70.