

Development of Algorithm for Improving Accuracy of Probability Coefficient of Threat Implementation in Personal Data Information

Sergey Verevkin^a, Ksenia Naumova^a, Tatiana Tatarnikova^a, Pavel Bogdanov^a and Ekaterina Kraeva^a

^aRussian State Hydrometeorological University, Voronezhskaya st. 79, St. Petersburg, 192007, Russia

Abstract

The continuing increase of the number of information systems inevitably entails the need to ensure cyber security of the information contained in them, in view of the need to provide both information containing commercial secrets and various types of information processed, including by State information systems. Considering the process of ensuring cyber security of the information, in the context of the need to comply with the requirements of legislative and regulatory acts, we should take note of the inevitability of creating a model of an illegal intruder and model of threats to the security of the protected information system, to determine the relevance of the vulnerabilities indicated in them. This article review the process of creating an algorithm that determines the existing methodology for determining actual threats to data security during their processing in information data systems, which is used at the step of building a model of security threats. The developed algorithm is relevant in view of its application to the current methodology, which serves as the main document in determining the requirements for the information security system. It is proposed to use a four-stage algorithm for collecting reconnaissance information from public sources (OSINT) for assessing risks and determining the state of security of an information system. The algorithm contains the steps of collecting information from freely distributed databases of supervisory authorities, external network resources of the organization, identifying potential an illegal intruder among the employees of the organization, as well as checking the organization's internal network resources. The developed algorithm is recurrent and allows organizing a recursive update of the input data collected as a result of its first execution, thereby providing data for a more detailed analysis when performing subsequent cycles. The information obtained as a result of OSINT analyze and provide to the managerial staff of the organization or the owner of the information system for further use in determining the appropriate coefficients of the current methodology.

Keywords 1

OSINT, corporate networks, security analysis, information security

1. Introduction

Today, a matter of necessity of the need to ensure the information security of the organization is increasingly arose not only by large corporations and government entities, but also by small private organizations. The main reason for it is the increase in the cost of processed information in the networks of organizations that has become the most desirable resource of cybercriminals.

Proceedings of the 12th Majorov International Conference on Software Engineering and Computer Systems, December 10-11, 2020, Online & Saint Petersburg, Russia

EMAIL: vrjovkin@rambler.ru (A. 1); ksenia.naumovaks@gmail.com (A. 2); tm-tatarn@yandex.ru (A. 3); 45bogdanov@gmail.com (A. 4); kate.smitt.by@mail.ru (A. 5);

ORCID: 0000-0002-5255-940X (A. 1); 0000-0001-6972-5390 (A. 2); 0000-0002-6419-0072 (A. 3); 0000-0002-7533-7316 (A. 4); 0000-0002-6938-1775 (A. 5)



© 2020 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

With the need to protect the information being processed, it is necessary to properly assess the current state of security of the information system in accordance with the requirements of current federal laws and other governing documents of supervisory bodies.

2. Justification of the existing problem

In carrying out the task of building an information protection system in organizations closely related to the processing of client databases that include personal data, an important point is the need to determine the current personal data threats when processing them in ISPD in accordance with the current FSTEC methodology [1].

As a result of the actions described in this methodology, employees of the organization are faced with the task of determining numerical coefficients Y_1 and Y_2 , which indicate the state of the initial security and the probability of the threat implementation.

Unlike the first coefficient determined by the table in the methodology, the value of the Y_2 coefficient should be determined by using the proposed verbal estimates corresponding to small, medium, high and unlikely.

It is worth noting the difficulty of conducting such assessments in the absence of any actual data on the current state of the organization's information systems and not to mention a further similar process for assessing the feasibility of a threat, which requires an impartial assessment of the possibility of implementing security incidents, including by the organization's staff.

3. Algorithm development

As a way to solve the problem of correctly determining the values of the Y_2 coefficient, we will build an algorithm that allows using open source software used for intelligence based on open information sources (OSINT) to search for existing threats.

Among the methods for conducting OSINT, the four-stage cyclic method for conducting data collection has gained the greatest popularity:

1. Definition of information search criteria
2. Retrieving searched data from open sources
3. Analysis of the received information
4. Structuring the obtained information in order to use it for further data search.

Therefore, the accuracy of the research conducted depends on the number of OSINT cycles, which allows you to determine the depth of analysis of the collected information depending on its type, secrecy and the wishes of the organization's management [2].

An important feature of OSINT is the full analysis of the organization's information and personnel resources. For this reason, we highlight three main steps of the algorithm being developed and consider the most successful methods of their implementation:

- 1) Analysis of public pages of the organization

It includes the collection and analysis of information about the organization posted in such sources of information, advertisements, organization websites, resources, tax information and other sources of information that allow you to obtain initial data on the activities of the organization: organizational structure, position, etc.

There are many software solutions, but as an example, we will consider the Maltego, which provides a convenient interface for visualizing data found and connections between it. Despite the fact that Maltego has a free version, the most effective are paid versions of the program that allow expanding its capabilities by connecting additional third-party libraries, the work of which is implemented by

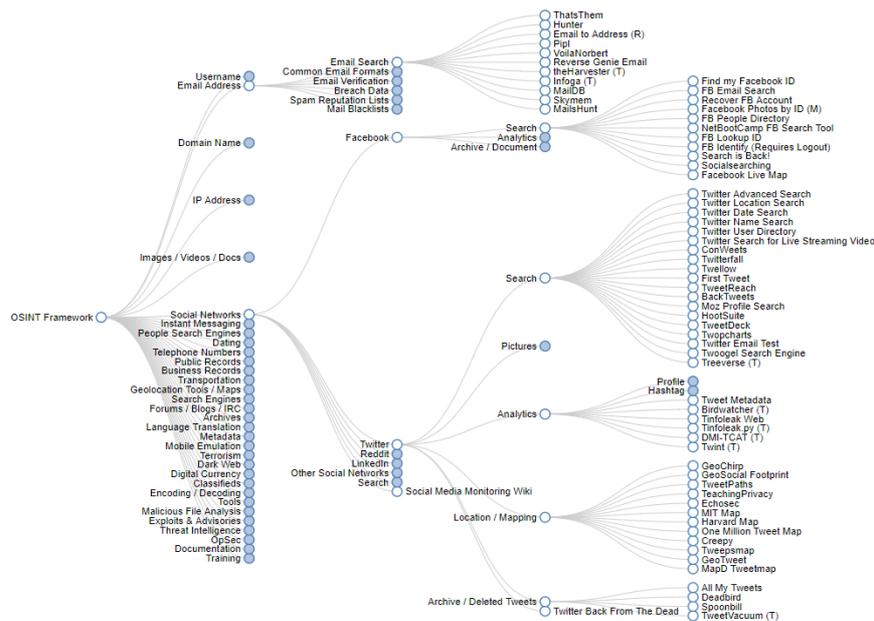


Figure 2: OSINT Framework solutions for finding information on popular social networks and e-mail services

An important task of this step is to identify dissatisfied employees who openly express dissatisfaction with colleagues and the organization as a whole. Often, it is a dissatisfied employee who is a potential victim of social engineers who provoke the employee to help achieve their own goals.

3) Analysis of the organization's network

The last but no least important step is to analyze the current state of security of corporate networks of the organization. In this step, it is important to analyze the network infrastructure used by the system and application software, the security tools used, protocols and other information that allows the abuser to plan attacks for specific network components.

The task of analyzing data about an organization's network can be solved in many different ways, the application of which depends on the type of network and the devices used in it. One of the most famous tools is Nmap. Using Nmap to the address found using Maltego IP, we can get information about the system software used, which is used on the hosting network resource. Figure 3 shows the result of the website rshu.ru hosting operating system definition.

```

ShellNo.1
File Actions Edit View Help
root@kali:~# nmap 85.142.104.52 -O
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-07 11:48 EST
Nmap scan report for webserver.rshu.ru (85.142.104.52)
Host is up (0.020s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
60020/tcp closed unknown
Device type: firewall|general purpose
Running: FreeBSD 6.X
OS CPE: cpe:/o:freebsd:freebsd:6.3 cpe:/o:freebsd:freebsd:6.2
OS details: m0n0wall 1.3b11 - 1.3b15 (FreeBSD 6.3), FreeBSD 6.2-RELEASE

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds
root@kali:~#

```

Figure 3: Definition of the website rshu.ru hosting operating system

The main criterion for choosing an implementation tool is to locate an attacker in relation to the network of the organization. If located in a segment of the corporate network, the use of sniffers to analyze network traffic for the use of vulnerable network protocols is needed. At the same time, for the

purpose of further penetration, it is necessary to use vulnerability scanners and Nmap analogues to search for vulnerabilities of border nodes of the network or to obtain information about the protection used in case of remote scanning of devices at the border of the investigated network in case of firewalls[4].

4. Conclusion

The result of the work is an algorithm, contributory factor to the process of determining the verbal coefficients of the probability of the implementation of security threats for information systems, through the use of the final report generated from the results of external OSINT and analysis of the organization's network. It should be pointed out the possibility of obtaining new data on threats existing in the information system, the identification of which in the case of multiple cyclical repetition of the algorithm contributes to the addition of the model of security threats and information created at the previous stages. Also should be pointed out that the developed algorithm can also be used when re-evaluating the security of an information system to identify new sources of threats and determine their relevance.

5. References

- [1] "Methodology for determining current threats to personal data security during their processing in personal data information systems" FSTEC of 14.02 2008
- [2] Penetration Testing Execution Standard (PTES), URL: http://www.pentest-standard.org/index.php/Main_Page
- [3] «Maltego Desktop Application Guide»URL: <https://docs.maltego.com/support/solutions/articles/15000008703-client-requirements#network-requirements-0-3>
- [4] Tatarnikova T.M., Volskiy A.V. Estimation of probabilistic-temporal characteristics of network nodes with traffic differentiation//Informatsionno-Upravliaiushchie Sistemy. 2018. V. 94 No. 3. P. 54-60. DOI 10.15217/issn1684-8853.2018.3.5
- [5] Tatarnikova T.M. Statistical methods for studying network traffic //Informatsionno-Upravliaiushchie Sistemy. 2018. V.96. No.5. P. 35-43. DOI: 10.31799/1684-8853-2018-5-35-43
- [6] Bogatyrev, V.A. Fault Tolerance of Clusters Configurations with Direct Connection of Storage Devices // Automatic Control and Computer Sciences - 2011, Vol. 45, No. 6, pp. 330-337
- [7] Bogatyrev A. V., Bogatyrev, V. A., Bogatyrev, S. V. Multipath Redundant Transmission with Packet Segmentation. In: 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), (2019). 8840647 doi: 10.1109/WECONF.2019.8840643
- [8] Bogatyrev, V.; Derkach, A. Evaluation of a Cyber-Physical Computing System with Migration of Virtual Machines during Continuous Computing. *Computers* **2020**, *9*, 42
- [9] Tatarnikova T.M., Dzubenko I.N. IoT system for detecting dangerous substances by smell// Informatsionno-Upravliaiushchie Sistemy. 2018. V. 93, No 2. P. 84-90. DOI 10.15217/issn1684-8853.2018.2.84