The infosecurity polygon concept

Ion BOLUN
Technical University of Moldova, Chisinau, Republic of Moldova

ion.bolun@isa.utm.md

Rodica BULAI
Technical University of Moldova, Chisinau, Republic of Moldova

rodica.bulai@ati.utm.md

Rostislav CĂLIN
Technical University of Moldova, Chisinau, Republic of Moldova

rostislav.calin@isa.utm.md

Abstract

In support of research/development in infosecurity in the Republic of Moldova, the PINFOSEC polygon is being implemented. The polygon will create the conditions and provide the necessary infrastructure and tools for conducting experiments/research/adaptations/developments, based on which practical recommendations will be elaborated and differentiated infomatics security (i-security) solutions will be proposed, taking into account the particularities of the republic. PINFOSEC concept defines basic objectives, determines functional structure, describes technological platform (SECIM), outlines SECIM modules and formulates principles of creating the system of infosecurity models (SIMOSI) for application as needed. SECIM modules will be implemented within the SIMOSI system, through simulations their characteristics will be researched, and further the afferent, depending on the case, i-security solutions will be developed to strengthen performances. Within PINFOSEC infospace, the INFOSEC website will be integrated. Its aim is to inform public administration institutions, economic agents, organizations and population about dangers, vulnerabilities, incidents, means and necessary actions of i-security and of other important aspects in the field. To begin with, the results of an incipient assessment of i-security state in enterprises/organizations/institutions (EOIs) are at the base of works within the polygon. These results are obtained by an

online survey using 24 indicators. According to this survey, the percentage of EOIs with high i-security performance for EOIs with over 500 employees is about twice as high as that for EOIs with up to 10 employees. It is estimated that PINFOSEC will significantly contribute to creating the necessary conditions for improving the i-security of EOIs and of population in the republic.

Keywords: *information security, infosecurity model, polygon functional structure, polygon platform..*

1. Introduction

Information is a strategic resource. Many parts of it are confidential (personal data, commercial secret, state secret). E-commerce is widely used, various online financial transfers take place, etc. Unauthorized access to such information, but also massive, targeted (as the case may be) misinformation of population, especially through Internet, leads to considerable losses, slowing down the pace of economic growth and population welfare. The estimates of International Monetary Fund [1] show that in 2015 they had losses due to cyber attacks approx. 32% of companies, and 18% are not sure that they did not suffer from such attacks. According to the impact, cybercrime ranks 2nd in various economic crimes [1]. Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion in 2021 [2] that is approx. 4% of global GDP. If in proportion to global losses, then in the Republic of Moldova they will constitute, starting with 2021, over 8 billion MDL annually. IT frauds causes losses of 0.5-5% of the total expenditure of public institutions [3]. The survey in the field of informatics security (i-security), conducted in Moldova in 2017 [4], showed that all users who use informatics means (i-means) need at least general knowledge in i-security. At the same time, in the period 2005-2014, the share of group organized cyber-attacks increased four times, reaching approx. 80% of the total [5]. Respectively, cyber-attacks are becoming more sophisticated, and counteracting them - increasingly difficult, requiring deep knowledge and related research. Applying local i-security solutions only temporarily reduces the risks. Moreover, the appropriate solution implemented today may in a relatively short time become insufficient.

The increasing severity of cybercrimes and the rising complexity of cyber-attacks accentuate the importance of research/development in i-security. It is required an overall approach to i-security with dynamic adaptation to concrete situations. The paper is intended to describe general aspects related to the destination, purpose, objectives, requirements, structure and functionalities of the PINFOSEC i-security polygon, as well as the platform and tools for its creation. First, an early estimate of the state of i-security in the Republic of Moldova is presented.

2. Informatics security state in the Republc of Moldova

At the moment, Moldovan official statistical data that would reflect the degree of i-security in the republic are not known [6]. The survey (23 questions), realized in

2017 under the Erasmus + LMPI project [4], was focused on identifying target professions and training needs on informatics security in Moldova and not on assessing the degree of i-security in the republic. At the same time, the Republic of Moldova appears in some international evaluations in the field (for example, Global Cybersecurity Index, GCIv3, 2018/2019 [7] and National Cyber Security Index – NCSI 2020 [8]), that show a slightly more advanced degree of infosecurity in Moldova than the international average.

The first trial to estimate the i-security state in Moldova was done in 2020 (May 25 - June 20) by an online survey [6]. Research was focused on EOIs. Five categories of EOIs were defined according to the number of employees (very small - up to 10 employees, small - 11-50 employees, small-medium - 51-100 employees, medium - 101-500 employees and large - over 500 employees), and each of them distinguishes between ICT-EOIs (EOIs related to Information and Communication Technologies sector - ICT) and non-ICT-EOIs (EOIs not-related to ICT sector). So, in total there were 10 categories of EOIs. For the incipient infosecurity state estimation, 24 indicators were used in the survey. The set of indicators was determined based on respective international practice, including that described in [7-10], and some limitations. The survey results are described in report [6]. Graphs of the dependence of ICT-EOIs (%ICT-EOIs) and non-ICT-EOIs (%non-ICT-EOIs) percentage on 23 indicators (indicators 3-26) are shown in Fig. 1.

From Fig. 1, it can be seen that the ICT-EOIs percentage in i-security varies from 34.1% to 94.1%. Only at 34.1% of EOIs is ensured high i-security performance in terms of IPS/WIPS use at all perimeter nodes of the EOI informatics network (indicator 15) and, likewise, the use of IDS/WIDS at all perimeter nodes of the EOI informatics network (indicator 14 - 35.2%). These two indicators are critical (the least EOIs have high i-security performance) for both ICT-EOIs and non-ICT-EOIs. A low degree of i-security is also in terms of testing external and internal penetration to identify vulnerabilities and attack vectors on EOI informatics space (indicator 22 - 59.1%), the use, in sensitive cases, of secure dedicated computers (indicator 7 - 68.2%) and performing the i-security audit of new informatics applications/systems before implementation (indicator 12 - 69.3%).

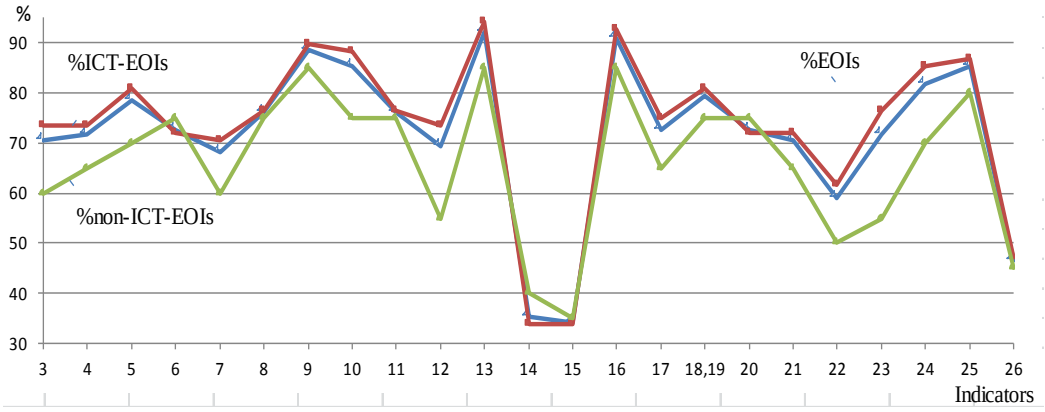

Fig. 1. The %EOIs, %ICT-EOIs and %non-ICT-EOIs dependence on indocators 3-26 [6].

The best situation regarding i-security is with the automatic creation of backups of sensitive information on secure servers (indicator 13 - 92.0%). A relatively high degree of i-security is also in terms of regulating access to resources (indicator 16 - 90.0%), the use of VPN (indicator 9 - 88.6%), the use of firewalls (indicator 10 - 85.2%) and informing employees about the implications of i-security, including possible malicious software (indicator 25 - 85.2%). Also, the unweighted average value of %EOI, %ICT-EOIs and %non-ICT-EOIs on the 23 i-security indicators constitutes:

- for EOI - 71.7%;
- for ICT-EOIs - 73.3%;
- for non-ICT-EOIs - 66.1%.

According to this survey, the percentage of EOIs with high i-security performance for EOIs with over 500 employees is about twice as high as that for EOIs with up to 10 employees (Fig. 2).

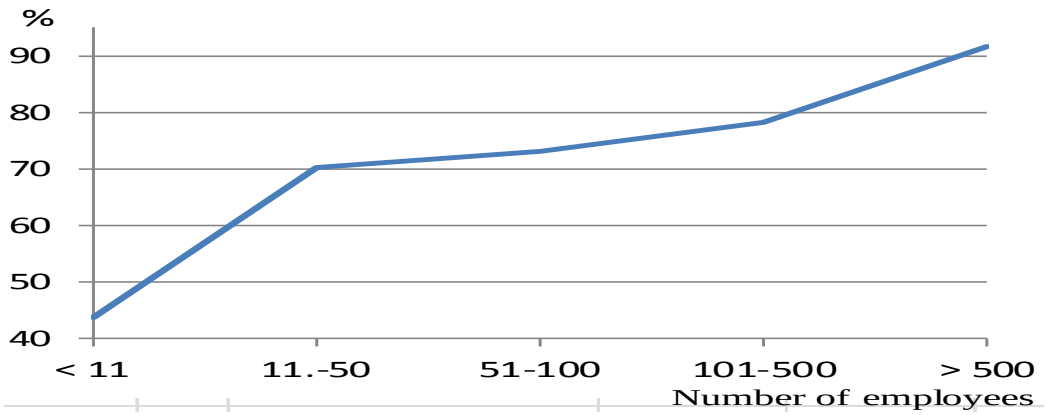

Fig. 2. The %EOIs average value (on indicators 3-26) dependence on the number of employees [6].

Thus, even according to this narrow set of 24 indicators (for example, the ETSI set contains 97 indicators [9], and the CIS one - 171 indicators [10]), it can be concluded that the state of EOIs i-security is relatively low, which confirms the need for additional measures in the field.

3. Destination, purpose and objectives of PINFOSEC polygon

PINFOSEC polygon is intended for experimentation, research, adaptation and development (ERAD-ment) of i-security solutions in support of needs of the Republic of Moldova. The purpose of launching the polygon is to create conditions, provide necessary infrastructure and tools for ERAD-ment and propose practical recommendations, solutions aimed to differentiated informatics securing, taking into account the Moldova particularities. The basic objectives regarding the PINFOSEC polygon consist in:

1. Creation of an extensible platform for the ERAD-ment of i-security solutions (SECIM).

2. Development of SECIM modules for the ERAD-ment of i-security solutions.

3. Development of a system of i-security models (SIMOSI) for application as needed.

4. Implementation of SECIM modules within the SIMOSI system, research through simulation of their i-security features and their development to strengthen performance.

5. Integration with the INFOSEC website for differentiated information of public administration institutions, economic agents and population regarding the dangers, vulnerabilities, means and activities on i-security, thus forming the PINFOSEC informatics space (i-space).

SECIM platform must form the technological support of ERAD-ed means of i-security. SECIM modules must be created as adaptations/developments of means of i-security. Based on SIMOSI i-security models, concrete solutions for differentiated i-security have to be generated, adapted to the needs of respective categories of entities in Moldova. The INFOSEC specialized website will facilitate the initiation in the field of EOIs and population and their target orientation in the diversity of information related to i-security.

4. Functional structure of the polygon

PINFOSEC i-space will be created as a secure virtual computer network (RINFOSEC) within the Techinical University of Moldova (TUM) i-infrastructure (Fig. 3). Within RINFOSEC, equipment can be used only within the PINFOSEC i-space. PINFOSEC means will be used to create, configure and emulate various informatics infrastructures and cyber incident situations, intended for the ERAD-ment of i-security means in accordance with objectives defined in section 3. Therefore RINFOSEC will include such i-means as: network stations, routers, switches, wireless access points, data transfer channels, transmission media, including wireless ones, i-tools, i-applications, specialized software, various information resources, etc. The basic technological solution of resource cooperation for exploring the PINFOSEC i-space will be a client-server one with five distinct categories of network stations (Fig. 3):

- PINFOSEC servers;
- PINFOSEC-Internet server that will host the INFOSEC website;
- Internet client stations - computers, smartphones, etc. outside the PINFOSEC i-space;
- PINFOSEC-Internet client stations - computers, smartphones, etc. outside the PINFOSEC i-space, but with restricted access to it;
- PINFOSEC client stations - computers, smartphones, etc. within the PINFOSEC i-space.

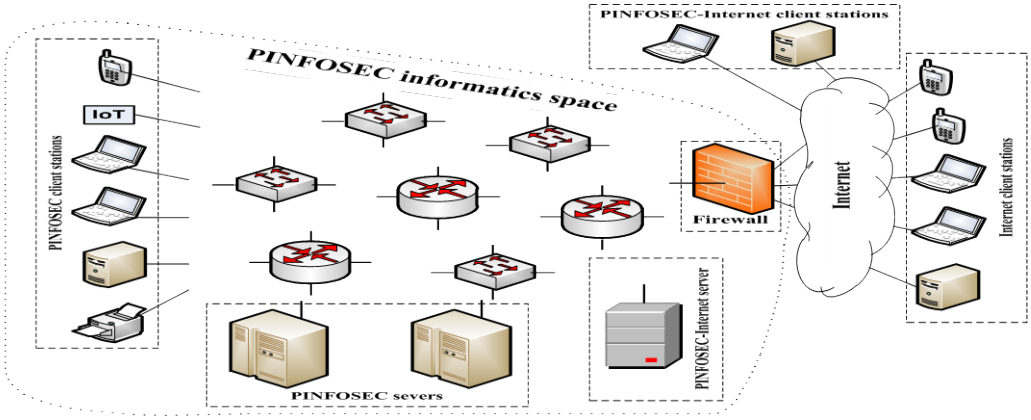

Fig. 3. PINFOSEC general funcţional structure.

PINFOSEC servers will be used for the ERAD-ment of i-security means. Their functions can also be performed within servers that perform other functions than those of PINFOSEC, within the i-infrastructure of TUM with the respective i-security. The PINFOSEC-Internet server (which will host the INFOSEC website) will serve both for Internet access of users to public information, and for some works of ERAD-ment of i-security means. Internet client stations (outside the PINFOSEC i-space) will be used to access the public information of INFOSEC website and, in part, to restricted access of some PINFOSEC resources through the INFOSEC website. PINFOSEC client stations (within the PINFOSEC i-space) will be used by users, depending on rights granted, for configuration, administration and ERAD-ment of i-security means. PINFOSEC-Internet client stations (outside the PINFOSEC i-space) will be used by users (Administrators and Operators) to access the public information of INFOSEC website and to restricted access of PINFOSEC resources through the INFOSEC website. If necessary, along with client-server technology, other technologies for network resource cooperation will be used.

Access to PINFOSEC i-space will be restricted. According to the level (rights) of access, three categories of users of PINFOSEC i-space will be distinguished: visitors, operators and administrators. For the three categories of users, two types of interfaces will be used: the PINFOSEC Administrator Interface - for administrator and operator users, and the INFOSEC Visitor Interface, also called Public Interface - for visiting users of INFOSEC website, including administrators and operators in quality of visitors. The Administrator Interface will be with limited access, authorization being obtained through a username, password and IP address of the access station, and the Public Interface will be with unlimited public access. So:

- Administrators constitute a distinct group of users who have unlimited access to the Public Interface of INFOSEC website and, through the Administrator Interface, to the Management System of PINFOSEC i-space;
- Operators constitute a distinct group of users who have unlimited access to the website Public Interface and limited access, through the Administrator Interface, to the Management System of PINFOSEC i-space. The rights and

access functions to PINFOSEC i-space Management System are defined by Administrators for each operator;

- Visitors are Internet users who have unlimited access to the Public Interface of
- INFOSEC website, and through this, possibly, to some PINFOSEC resources.

In other words, all users, including Visitors, will have access, through the Public Interface, to the content of INFOSEC website, and Administrators and Operators will have access, through the Administrator Interface, to the PINFOSEC i-space Management System. In order to increase the security of PINFOSEC i-space, Administrators and Operators must be able to access the PINFOSEC i-space Management System only from certain computers, obtaining for this purpose an additional authorization, in addition to name and password, after the IP address of the computer, from which the access in question is attempted. Upon entering the system, depending on the nature of access, the system will display to the user either the Public Interface or the Administrator Interface. Visitors must also be able to access via the FTP service to copy very large content files from INFOSEC website. As client computers, when accessing the resources of PINFOSEC i-space, can serve the Visitors computers and also the Administrators computers and those of Operators. The access to Internet Server of PINFOSEC i-space will be made:

- for users - from any computer with Internet access;
- for administrators and operators - from certain computers in the TUM Informatics Network and, if necessary, a small number of other stations with Internet access.

The network interconnection of Internet and PINFOSEC-Internet client stations and of PINFOSEC-Internet server will be performed through Internet, and within PINFOSEC i-space will be performed through means of TUM Informatics Network, using routers, switches, transfer data media and, if necessary, other equipment. The infrastructure of PINFOSEC i-space will be reconfigured, depending on the investigated i-security means. The performance required for client stations used by PINFOSEC users depends on resource requirements of operating systems and applications used to access PINFOSEC resources and to receive, store, and render responses to requested requests. Thus, there are no special performance requirements for Internet client stations. For PINFOSEC-Internet and PINFOSEC client stations, these requirements also depend on specialized software to be researched, the experiments to be performed, but, initially, special performance requirements are not also submitted. Obviously, running applications with advanced graphics or video will require respective performances at client station used for this purpose (VRAM memory capacity, processor productivity, etc.). Of course, the main focus is on PINFOSEC-Internet server and PINFOSEC servers. The specificity of PINFOSEC-Internet server consists, first of all, in the fact that it will contain a relatively voluminous Database and File System; secondly, it is intended to serve a wide range of users online in real time. Special resources may be required in some research for PINFOSEC servers as well. At the same time, in order to ensure the minimum reliability requirements, it may be appropriate, in some cases, to use the reservation of resources.

5. Some PINFOSEC polygon functional aspects

As mentioned in Section 3, SECIM platform will form the technological support of i-security means that will be ERAD-ed within the PINFOSEC polygon. SECIM modules will be adaptations/developments of some means of i-security. They will be developed using as a starting point, for example, the CIS Controls set of actions/sub-controls [10] or similar, including those aimed at meeting the performance requirements, as measured by the ETSI Ifomation Security Indicators [9]. Based on SIMOSI i-security models, concrete differentiated i-security solutions will be generated, adapted to needs of various categories of entities in Moldova, considerably facilitating the respective activities and, at the same time, strengthening the expected effects. The SECIM platform extensibility will allow the resultant continuation of the ERAD of i-security solutions in rhythm with the advancement of theoretical results and of practical means in the field.

Within PINFOSEC polygon, such means could be implemented/researched as:

1. Vulnerability management systems (vulnerability knowledge base, connected to such international vulnerability databases as: https://nvd.nist.gov/, https://vuldb.com/, https://www.cvedetails.com/, https://www.exploit-db.com/, https://www.rapid7.com/. Vulnerability detection and prioritization, automation and efficient integration with existing security infrastructure and processes - (*Vulnerability Manager*).

2. Real-time event monitoring and management tools for detecting threats and vulnerabilities. Correlation capabilities to identify fraudulent schemes and abnormal user activity. Traffic analysis to detect threats that cannot be detected by standard tools, such as IPS/AV/Firewall - (*SIEM*).

3. Models/instruments with penetration tests. Ability to simulate attacks and prioritize critical resources for protection.

4. Security risk identification and prioritization systems to help reduce threat exposure and the risk of data loss, information risk management. Risk analysis associated with the human factor - Human Risk Analytics. Models of Security Risk Analysis Methodologies according to ISO 27005, NIST 800-30, such as BSI IT-Grundschutz (Germany), Mehari and Ebios (France), CRAMM (United Kingdom), etc.

5. Tools for reporting the conformity of security systems to comply with the requirements of national and/or international regulations (GD RM 201, ISO 27001, ISO 22301, ISO 27017, CIS Controls, PCI DSS, GDPR, NIST, OWASP, etc.) or their violation.

6. Models for identification and selection of control measures. Analysis and integration of best practice frameworks, combining COBIT 5, PCI DSS, ISO 2700k, NIST SP800-53, CSI and GDPR to ensure a comprehensive security approach. Elaboration and monitoring of identified risks treatment plan (*Risk Manager*).

7. Template packages for SIMOSI: context, security requirements and objectives, policies and procedures, nomenclatures with assets, vulnerabilities and threats, etc. (*Toolkit*).

8. IT tools and techniques regarding the audit activity in i-security (*SecAudit*);

9. Automation of i-crime investigation techniques - (*Digital forensics*).

10. Educational platform - a special environment for training, awareness programs, training of hacking skills, etc. (*EduSec*).

INFOSEC website will ensure the prompt information of EOIs and population on vulnerabilities, risks, means, incidents and actions of computer security and other important aspects in the field, including their target orientation in the diversity of online information related to i-security.

6. Conclusion

The concept addresses the major aspects related to elaboration, implementation, maintenance and development of PINFOSEC polygon, starting from the definition of purpose, objectives and basic requirements towards it and to the elucidation of respective strategic technological solutions. PINFOSEC polygon will significantly contribute to the creation of necessary conditions for improving the security of informatics resources of enterprises, organizations and public administration institutions and those of population in Moldova. At the same time, the conditions for training of highly qualified young specialists and for the continuous training of specialists in informatics security and information technologies in general will be improved.

References

[1] International Monetary Fund (October 2016), World Economic Outlook: Subdued Demand: Symptoms and Remedies, Washington, USA.

[2] *2019 Official Annual Cybercrime Report*, Cybersecurity Ventures (2019), https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf (accessed 24.09.2020).

[3] *Guide to Understanding the Total Impact of Fraud* (February 2020), International Public Sector Fraud Forum, https://assets.publishing.service.gov.uk/government/ uploads/system/uploads/attachment_data/ file/866608/2377_The_Impact_of_ Fraud_ AW__4_.pdf (accessed 12.02.2020).

[4] Bolun, I., Beşliu, V., Rusu, G., Negară, C. (2017), *Sondaj de identificare a profesiilor ţintă şi a nevoilor de instruire în domeniul securităţii informatice în Moldova*, Chişinău, https://www.lmpi-erasmus.net/en/project.aspx (accessed 25.08.2019).

[5] Ablon, L., Libicki, M.C., Galay. A. (2014), *Markets for Cybercrime Tools and Stolen Information: Hackers' Bazaar*, Rand Corporation.

[6] Bolun, I., Ciorbă, D., Zgureanu, A., Bulai, R., Călin, R., Bodoga, C. (2020), Report "*Starea, necesităţile şi priorităţile securităţii informatice în Republica Moldova*", Chişinău, UTM.

[7] *Global* Cybersecurity *Index 2018* (2019), ITU, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (accessed 15.02.2020).

[8] *National Cyber Security Index* (2019), eGovernance Academy, Tallin, Estonia, https://ncsi.ega.ee/ methodology/ (accessed 14.02.2020).

[9] *ETSI GS ISI 001-1 V1.1.1 (2013-04) Information Security Indicators* (2013), ETSI, https://www.etsi.org/deliver/etsi_gs/ISI/001_099/00101/01.01.01_60/gs_isi00101v010101p.pdf (accessed 21.02.2020).

[10] *CIS Controls v. 7.1 Measures and Metrics* (2019), Center for Internet Security, https://www.cisecurity.org/white-papers/cis-controls-v7-measures-metrics/ (accessed 24.02.2020).