BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 2. SZÁM

The protection of pension payment systems, as critical infrastructure

Zsolt Szabó
Doctoral School on Safety and Security Sciences, Óbuda University, Budapest, Hungary
zsolt@tamiyaryu.hu

***Abstract* — Nowadays information is one of the most valuable assets in the economy and society. Information is a resource for organizations, the basis for efficient operation, and an asset of the organization, therefore, it is extremely important to protect data. There are processes that can cause a critical situation in the organization in the case of a problem, if they are not controlled properly and if we do not take the proper precautions to avert disaster. The operation of the state pension payment system and the data it manages are governed by law, therefore their protection is of paramount importance. The study consists of three parts. The first part summarizes the information security threats threatening pension payment systems and presents the possible ways to counter these threats. The second part examines the planning of business continuity, with special attention to risk management and business continuity management. The third part provides a possible guideline for pension payment systems to help them comply with the new European General Data Protection Regulation.**

***Keywords*: Pension payment systems, planning of business continuity, GDPR**

1 INTRODUCTION

The protection of critical infrastructure is a challenge of the present time, which receives more and more attention worldwide as global terrorism spreads. Critical infrastructure is infrastructure on which a society, an economy relies on to be able to function. Protecting critical infrastructure is especially important nowadays, in the time of 4GW or asymmetric warfare, when almost any group can enforce its demands using cyberwarfare even against much larger enemies, typically nation states. The main target of attacks is critical infrastructure (CI), especially critical information infrastructure (CII). A state uses critical infrastructure to store the data of its citizens, to operate its public administration (not only e-public administration) and to provide services to its citizens (not only e-governance). Therefore, it is the state's responsibility to protect this infrastructure, especially because the state relies on this infrastructure, too. If any element of critical infrastructure breaks down, it can push the nation state into chaos and anarchy. Therefore, the state has to concentrate on executing the tasks accurately and continuously maintaining protection.

2 INFORMATION SECURITY TRENDS THREATENING PENSION PAYMENT SYSTEMS

Nowadays the state, all its organizations and citizens are vulnerable to the extremely complex electronic information systems in the cyberspace of Hungary, without which the state cannot operate and the various services cannot be provided. Society is not prepared to operate without the lost infrastructure, tools or services, therefore these have to be protected, especially because the information and data generated during their operation represent considerable value. The target of attacks is primarily the data, which is surrounded by various system elements and processed by processes [1]. Cyber threats threaten data and the processes handling these data through a definite chain of system elements. There are usually three kinds of malware: scareware; programs that steal money or data that can be sold; and government level spyware, cyberwarfare [2].

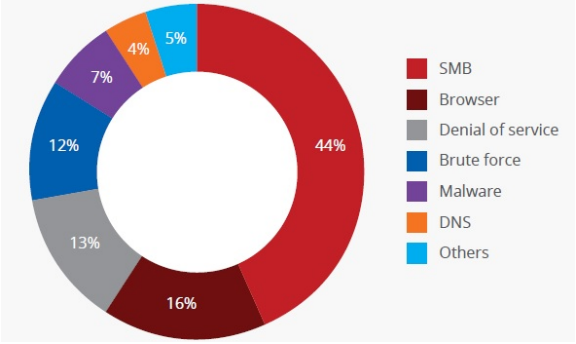

Figure 1: Top network attacks in Q3 [3]

Based on Fig. 1 intentional damage is more and more common, and at the same time, the attacks are more and more daring and complex [4]. The threat is increasing and cyberterrorism is a danger to our vulnerable information systems, such as the pension payment system [5].

In Hungary, pension payment tasks are carried out by the Pension Payment Directorat. Pension payment belongs in the group of financial services. Fig. 2 shows that critical payment processes belong to communication between banks: national (VIBER) and international (GIRO, SWIFT) payment systems. One of the vulnerabilities of these systems has recently been highlighted by the Shadow Brokers hacker group: the attackers used zero-day vulnerabilities stolen from National Security Agency (NSA) of the USA, and published by the Shadow Brokers. These vulnerabilities were spread by old, not supported operating systems (Windows XP and Windows Server 2003). The reports of the network of the EastNets Service Bureau (ENSB), allegedly threatened by the hackers, are incorrect and unfounded. The internal security unit of EastNets Network performed a comprehensive security check on its servers and found no vulnerability or data compromised by hackers.

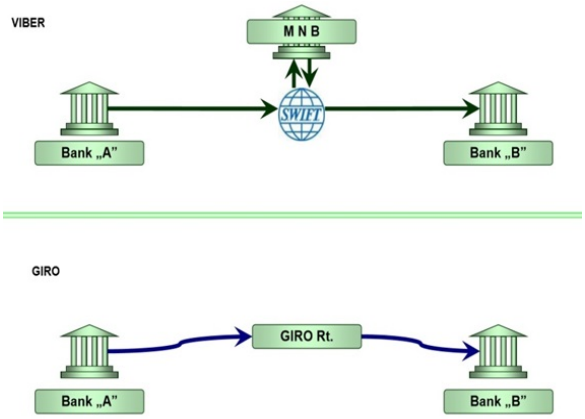

Figure 2: National/Foreign payment system [otpbank.hu]

Based on the international example mentioned earlier, the elimination of any of the electronic information systems or services can affect a large part of society. Furthermore, the confidentiality, integrity and availability of the data handled by these electronic information systems is of paramount importance. Its legal and institutional background is provided by Act L. of 2013 on the electronic information security of state and local government organizations (Ibtv.) and the related regulations [6] [7].

ESET Trends 2017 [8] Security held ransom predicts: 2017 will be the year of Ransomware of Things (RoT)! ESET Research Laboratories has collected data from all over the world and the data suggest that 2017 will be even more the "year of ransomware". The report says that a new trend is emerging, Ransomware of Things (RoT), which means attackers break into our devices, block our data, then demand a ransom to unblock access to the data. This is a new form of crime: through IoT (Internet of Things) the hackers can block any of the connected devices. This can even be a car, when the hackers can "lock" the car if it is connected to an application on the mobile phone of the user, because they can access the telephone and through the telephone, they can block the starting of the car. Then they can demand ransom in a text message. Further threats are forecasted and strengthening the protection of our information systems is more and more important. In the case of electronic information systems, the immediate detection of security events (Fig 1) is especially important. These are unwanted or unexpected events or series of events which cause a change in the electronic information system as a result of which the confidentiality, integrity, credibility, functionality or availability of the data is damaged or lost. If the security event occurs, it is very important to handle it. This means documenting the event, repairing the damage, finding the people responsible and preventing the future occurrence of the event.

The report titled "Cybersecurity Trends 2018: The Cost of our Connected World" compiled by ESET security experts, presents topics that will be of interest to everyone following an increase in, and sophistication of, cybersecurity incidents in 2017 [9]. The report focuses on ransomware, attacks on critical infrastructure, malware and combating criminal activity, as well as the cyber threats posed to electoral campaigns and data privacy. The General Data Protection Regulation comes into force in May 2018, replacing the Data Protection Directive and increasing the legislative concern surrounding data privacy. In the report focuses on user-awareness of data collection, the risks faced by data collected through the Internet of Things (IoT), and the significant fines for companies that fail to protect personal data. Technological innovations and their use in 2017 have produced remarkable possibilities in the digital world, while also exposing users to new kinds of threats. This year we have seen cybercriminals focus their attacks on sensitive and private information. 2018 is the year users need to increase their awareness of cyber threats and manage their digital world more responsibly. Cybersecurity will be of great importance for not only enterprises but for private people as well. In addition to the protection of traditional computer devices – computers, tablets, smart phones – more and more attention will have to be paid to the protection of various IoT devices, since hackers try attacking new technologies more and more often.

3 THE SECURITY ISSUES OF ELECTRONIC ADMINISTRATION

The Electronic Administration System (Document Gate) of the Central Administration of National Pension Insurance (ONYF) makes it possible for users to manage their problems on the Internet. Users that have access to the Government Portal Customer Portal can fill in and submit electronic forms. With the provision of this service, ONYF wishes to comply with the general rules relating to administrative procedures and services satisfy the needs of customers. The Document Gate has the following three main functions:

1.) Handling electronic signatures: The Document Gate comprehensively handles electronic signatures as required by law, their creation, verification, and the handling of time stamps or the equivalent time marks.

2.) Secure document transfer: the Document Gate system provides a single-gate transfer channel between the customer and the systems of ONYF to send and receive documents, as the law allows it.

3.) Customer identification: The Document Gate system is able to identify the customer based on the customer database of ONYF, through the identification service of the customer portal.

The Document Gate system ensures that the communication between the customers and customer service reflects the structure of the organization of ONYF, which can be divided into two main levels shown in Fig. 4:

Level A: central organizational unit (ONYF), and under this

Level B: the pension payment directorate (NYUFIG) and regional organizations (NVI).

The hierarchy of the communication between the organizational units of ONYF: the documents arriving from the customers – Web forms, attachments – are received by the single-gate Document Gate system. The Document Gate system generates the arrival number and pre-sorts the documents (based on address and the type of the filled form). The pre-sorted documents are transferred to the individual organizational units. Customer service assistants do not get emails from customers. ONYF's replies from the individual organizational units are collected by the Document Gate system and sent to the customers.

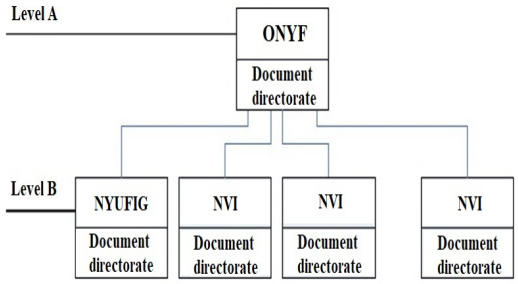

Figure 4: The hierarchy of the communication between the organizational units of ONYF [onyf.hu and own figure]

The most obvious security issues of the Document Gate system are the websites, since these are the most visible; they suffer the most attacks. After a successful attack, all traffic passing through the portal can be monitored, and the compromised system can be a stepping-stone to internal, protected systems [10]. This is why the vulnerability check of web servers and web applications is very important, with the recommendations of OWASP TOP10 taken into account, that is, the 10 most critical defects in web applications. Below are a few basic security requirements with which risk can be decreased: Web servers should be hosted in our own DMZ or a webhosting provider. The web server should be a dedicated host; it should not run other services or virtual servers. The proper operating system should be chosen and it should have reinforced and updated security. The software on the server should be updated regularly. Strong authentication should be used wherever possible. All unnecessary writing, reading and execution rights should be blocked. The portal should be on a separate partition. All other services should be blocked on the server. All documentation showing the operation of the portal engine should be removed. All default or test files should be deleted. The server process should have limited rights. Do not allow file uploads through the portal. Be careful about temporary files that are generated during running. Pay extra attention to making sure that classified documents are not available on the portal. All activities should be monitored and logged.

4 Compliance with the new European General Data Protection Regulation

On 4 May 2016, the final text of Regulation 2016/679 of the European Parliament and Council (hereinafter called the General Data Protection Regulation) was published in the official journal of the European Union [11]. This was the last step of the data protection regulation reform of the EU. Although the Regulation enters into force 20 days after publication, that is, on 25 May 2016, it only has to be applied from 25 May 2018. Data handlers, data processors and national codifiers therefore got a preparation time of two years to comply with the regulations and requirements of the new European data protection regulation, of which less than only 8 months have remained now. The General Data Protection Regulation replaces the current 95/46/EK Data Protection Directive and brings significant changes in this legal area. One of the most important changes is in the form of regulation: the moderate approach, which meant the member states were allowed to determine their data protection requirements based on the guidelines of a directive, is replaced by new Regulation, which will be directly in force and applicable in all the member states. This will result in uniform data protection regulation all over the EU, and more predictability for companies managing data in several states – although some national specialties can remain. The new Regulation further extends the rights of the stakeholders and the authority of the national data protection authorities, increases the responsibility of data handlers and its authority can at times extend beyond the borders of the EU.

The current study examines the issue of "Reporting a data protection incident". The Privacy Act currently states an obligation to record the incident in order to check the measures related to the data protection incident and to inform the affected party. The record contains the affected personal data, the people affected by the incident, the time, circumstances and effects of the incident, and the measures taken to eliminate it, and other data as required by law. At the request of the affected party, the data handler informs them about it. According to the new regulation, if personal data is handled or processed unlawfully, it has to be reported to the supervisory authority. The data handler reports the data protection incident to the supervisory authority without undue delay, if possible, within 72 hours after they learnt about the incident, except if the incident probably does not pose a risk to natural persons' rights and freedoms [11]. The obligation to report data security incidents is justified and does not put disproportionate load on data handlers.

There are more and more IT security incidents in the news, in which the information security of an organization is compromised, data is stolen or systems are crippled by attackers. The IT security of these systems were not good, there were vulnerabilities that the attackers were able to exploit. The question arises:

- What is good IT security?
- Could the affected companies have prevented these attacks if they had paid more attention to and spent more money on data security?

The point of IT security is to prevent these kinds of attacks. Since companies have to prepare for a possible incident, many company leaders consider the cost unnecessary and only install minimal security required by regulations and the law. In addition to high cost, it also makes creating a secure system difficult that often the primary objectives are the functionality and usability of the system, while security is a secondary goal. The primary goal is always to ensure the market success of the company and the task of the IT infrastructure is to support this as much as possible. However, if due to inadequate IT security, confidential information – such as customer data, business secrets, strategic plans – becomes public, it can not only endanger success but can lead to the fall of the company. This is why it is important that companies have a risk management plan, in which with the help of risk assessment they can assess the probability of occurrence of a threat and the resulting damage. Using this information the management can decide whether it accepts the risk or reduces or eliminates it.

There is no complete security. Day by day vulnerabilities are discovered. (Hardware and software problems and problems resulting from the improper configuration of the devices of the IT system are collectively called vulnerabilities.) Microsoft shows a good example of handling these – they publish updates for their products on the first Tuesday of every month. If these are not installed, our system will contain known vulnerabilities.

Vulnerability scanning software helps find vulnerabilities and assess the risk they pose.

The key to defence is Time to Detection (TTD) – this is the most important conclusion of the Cisco Midyear Cybersecurity report [12]. Cisco has been tracking our median TTD since November 2015. Since that time, the overall trend hasbeen downward-from just over 39 hours at the start of our research to about 3.5 hours for the period from November 2016 to May 2017 (see Fig. 5).

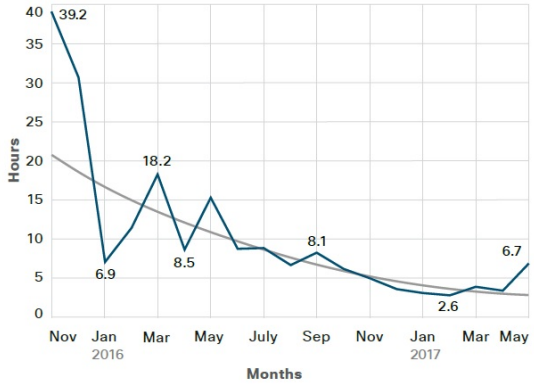

Figure 5: Median TTD by month [cisco.com/go/mcr2017graphics]

Defence requires integrated solutions, such as SOC – Security Operations Center (Fig. 6) and SIEM - Security Information and Event Management (Fig. 7), which are far more effective than endpoint security.

It is also more and more important that companies (users) cooperate with reliable manufacturers. Such manufacturers can help with expertise, guidance, and if necessary, they can assess the risk of organizations, too.

Risk monitoring has many solutions and techniques. For example, these techniques can filter events and call attention to only the few events which are likely incidents. And they do not only reduce the number of events worth looking at but also rank them according to risk so that human resources can be better allocated. The investigation of incidents ideally has to happen in real time or with little delay. General information collection can effectively help the detection of differences from normal operation. The above can be performed with a SIEM system, for example, which logs and analyses the reports, alerts and warnings generated by software and hardware tools and devices. The abbreviations SIM and SEM also appear in the literature, and they are often mixed up with SIEM, because they are used for similar purposes.

The purpose of SIEM and similar systems is to store and analyze events centrally, thus ensuring that security events are detected. Other technical tools can support human resources but they have to be based on strong control and regulated processes. It should be regulated that if an event occurs, what should be done and who should do it.

Figure 6: Components of SOC [nuspire.com/technologies/soc/]

Therefore, the incident management process has to show what has to be done in an event-controlled environment. And when this alert is activated, a response has to start. Obviously, it should be in harmony with many other processes, such as the business continuity plan or the disaster recovery plan. The harmonious cooperation of these and other processes can effectively support incident management with the help of processes and technical devices.

Figure 7: Typical features of SIEM [mita.gov.mt]

Information security incident: an information security event or series of events which adversely affects information security controls (defence measures), and/or involves the circumvention of information security rules and settings, and/or affects availability or business continuity to such an extent that it is considered a crisis.

Any unexpected event affecting the critical key processes of the Organization can be called a crisis if

- one or more resources used by one or more critical key processes (human, facility, IT etc.) are not available, and
- as a result of unavailable resources, the basic tasks of the Organization or organizations using the IT services of the Organization are threatened or cannot be done and
- the unavailable resources and services cannot be recovered in the maximal tolerable downtime with the available resources and tools in normal operation and
- if recovery was performed with the resources and tools in normal operation, during the period of

recovery the Organization would suffer intolerable material, moral or legal damage.

Information security events become information security incidents after they are qualified as such, as the criteria of incidents have to be examined, and the level of tolerance can be different in different information systems.

5 STEPS OF MODELLING AN INTELLIGENT IT SECURITY SYSTEM

The modeling process described above is applied to the to designing and building intelligent IT systems, which provide, without embodying actual (human) intelligence, various information security services and solutions. Information is important for all economic entities, be it a state or private organization.

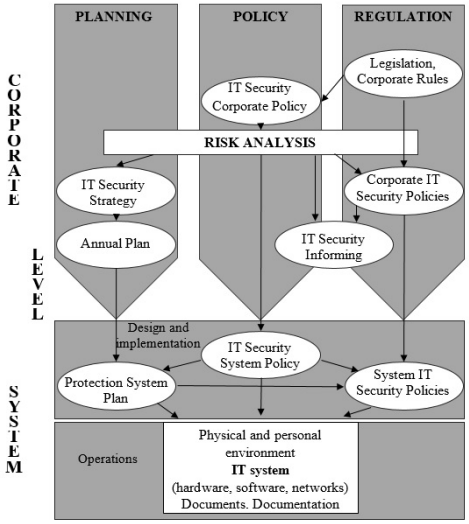

Figure 8: The process of implementation of IT protection [own figure]

Without information there is, no progression, no chance for planning- lack of it results in fallback, regression [13]. Information a resource for organizations, the basis of efficient operation, an asset of the organization and often a product, which is why it is necessary to ensure that it is preserved and protected. IT security means maintaining IT components of organisational activities in a satisfactory condition in order to achive goals [14]. Security is one of the essential elements of organisational operation, in the case of a state-run pension paying agency it is of the same priority as the organizational conditions [15]. Attacks are primarily aimed at obtaining the data surrounded by various system components, managed constantly [16]. The possible threats endanger data through the determined chain of system elements, processes managing data and databases [17]. The implementation of protection does not only mean the implementation of a set of tools, rather a process that spans from planning to implementation, covering the physical (operation), logical (password generating methods, cryptographic processes, incompatibility matrix), administrative (regulatory background) and human resources protection systems of the relevant organization [18].

All organizations set up goals defined in organizational strategy. IT strategy aims at surveying of IT applications essential for reaching the organization's goals. The IT strategy of an organization is always part of the organizational strategy. The steps of shaping the limitational, strategy developmental, planning-realizational and controlling-implementary capabilities of IT security should be planned and executed in accordance to the IT planning cycle. The two projects can run in parallel. Their common elements can be handled together, their partial results can be used and they can reach the goals in conjunction the organization is aiming at. Security strategy is a very important component of organizational strategy as well. The term „security" means a condition in which the operations of the organization can be done without confusion. A system responsible for the operations of an organization should cover all operations touched by the organizational strategy (see Fig. 8). Organizational and IT strategy insures exhaustiveness and integrated level of security together, hence IT security is essential part of the IT system and security system on organizational level. An IT security system needs solutions that meet security requirements with as small as possible tolerable risks having been taken into account. Setting up the planning and the administrative defense concepts of IT security system (i.e. the physical, logical and human defense system) should be a part of every IT project [19].

The organization of the security is a complex concept, the individual component areas are closely related and depend on one another. Development of an IT security concept of a state-run pension paying agency is essential, since it belongs to the scope of critical infrastructure. The establishment of IT security for state agencies is guaranteed by the conditions of meeting the IT security and protection provisions contained in Act L of 2013 (Ibtv.) [7], the implementation of a complex, efficient security system compliant with the expectations of the law, which can be maintained at a low cost in the medium and long term. State IT systems must comply with Act L of 2013 and Lrtv. efforts must be made to accomplish the necessary and sufficient level of security, while ensuring the continuous regular operation of the given security system. It is a justified expectation from agencies maintained by the central budget that they implement, sustain and operate their IT security systems in a cost-effective way and at the highest level of protection that is available in our time. The security system should be built up from individual and group – block – module elements, which rely on one another, then the individual groups should be observed, operated in a cost-efficient way and logged from one point. The individual tasks consists of modules that constitute parts of the large units. Security tasks can be divided up into three large groups (see Fig. 9):

1. Infrastructure security framework: its function is to create a common security environment for all systems.
2. Application security elements: they provide protective elements for the individual application development projects.
3. Management and monitoring system: a sub-system serving the operation and control of the previous two groups.

The simultaneous operation of the first two systems ensure compliance with the security laws, decrees and regulations, i.e. in themselves they are not sufficient for meeting the conditions.

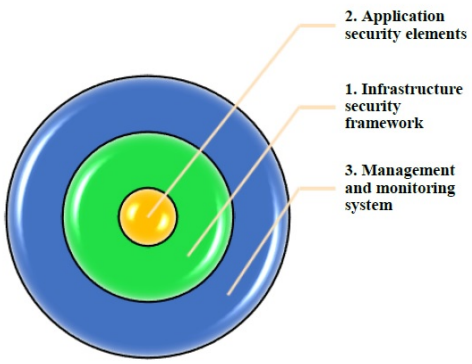

Figure 9: Security system groups [own figure]

The third system enables proper operation. The implementation of the system should be scheduled as follows:

1. Establishment of the security framework infrastructure (this serves as the receiving environment for the rest of the elements).
2. Build-up of the management and monitoring system.
3. Bringing into service of the application security elements in the system.

Considering the above details, the protection to be implemented must be closed, comprehensive, proportionate with the risks and provided constantly in time. Efforts must be aimed at the establishment of the management of security of the IT system of an organization, its centralization, the provision of support to it in a transparent manner by IT tools and its automation at the highest possible level, eliminating the human factor as much as possible [16]. It is a legal requirement that the IT system of state agencies must be capable of monitoring and logging the critical security events of determining importance for the operation of the agency and the automated management of such events [7] [11].

6 Conclusions

Nowadays state organizations have to pay special attention to information security, because protecting confidential information, and ensuring its integrity and availability are of paramount importance. Information security should not be regarded as merely prevention, rather much more as a comprehensive strategic issue. Companies often try to cover information security with IT security but it is not a single-factor task, but a very complex process. This study collected the factors which should be considered when building the highest level of information security in a company. In our days planning a complex IT security system requires the possession of skills and application of up-to-date planning methodologies. As the study shows, a high number of aspects must be taken into account in the planning of both areas in order to ensure the success of these efforts.

REFERENCES

[1] Zs. Szabó (2017): Cybersecurity issues of pension payments. In: Szakál Anikó (szerk.). IEEE 15th International Symposium on Intelligent Systems and Informatics: SISY 2017. Subotica, Serbia. 2017.09.14-2017.09.16. New York: IEEE. pp. 289-292.

[2] M. Russinovich (2011): Zero Day: A Novel. Thomas Dunne Books, March 15, 2011. pp. 1- 350.

[3] McAfee (2017): McAfee Labs Threat Report, December 2017. https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-dec-2017.pdf (Downloaded: 16/04/2018)

[4] B. Albert - László, J. Frangos (2002): Linked: The New Science Of Networks Science Of Networks. Basic Books. pp. 1-288.

[5] M. Russinovich (2012): Trojan Horse. Thomas Dunne Books. September 4, 2012. pp. 1- 380.

[6] T. Szádeczky (2015): Information Security Law and Strategy in Hungary, Academic and Applied Research in Public Management Science 14:(4). pp. 281-289.

[7] Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény (Ibtv.). Magyar Közlöny 2013. évi 68. sz. pp. 50241-50255.

[8] ESET (2017): Trends 2017 Security Held Ransom. https://www.welivesecurity.com/wp-content/uploads/2016/12/ESET-Trends-2017-security-held-ransom.pdf (Downloaded: 15/10/2017)

[9] ESET (2018): Cybersecurity Trends 2018: The Cost of Our Connected World. https://www.welivesecurity.com/wp-content/uploads/2017/12/ESET_Trends_Report_2018.pdf (Downloaded: 17/04/2018)

[10] Zs. Szabó (2017): The Information Security and IT Security Questions of Pension Payment. In: Lucia Figuli, Pavel Manas, Alexander N Kravcov, Václav Pospíchal, Bohuš Leitner, Pavel Svoboda (editor) Structural and Mechanical Engineering for Security and Prevention: ICSMESP 2017. Prague, Czech Republic. 2017.06.14-2017.06.16. Prague: Trans Tech Publications. 2017. pp. 322-327.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Downloaded: 17/04/2018)

[12] CISCO (2018): Cisco 2017 Midyear Cybersecurity Report https://www.automation.com/pdf_articles/cisco/Cisco_2017_MCR_Embargoed_til_072017_5_AM_PT_8_AM_ET.pdf (Downloaded: 18/04/2018)

[13] Á. Csiszárik - Kocsir, J. Varga, Crisis (2017): Project - Risk: According to the Opinions of Hungarian SMES, Project Management Development - Practice and Perspectives: Sixth International Scientific Conference on Project Management in the Baltic Countries. pp. 60-70.

[14] Dornfeld, L. - Keleti, A. - Barsy, M. - Kilin, J. - Berki, G. - Dr. Pintér, I. (editor) (2016): Geopolitics of the Virtual Space. Geopolitical Council. Budapest. 2016/1. pp. 1- 369.

[15] P. Michelberger, Cs. Lábodi (2012): After Information Security - Before a Paradigm Change: A complex Enterprise Security Model. Acta Polytechnica Hungarica 9:(4). pp. 101-116.

[16] Zs. Szabó (2016): Options of micro-simulation in the modelling of the pension system and the intelligent IT security system. Computational Intelligence and Informatics (CINTI), 2016 IEEE 17th International Symposium on Óbudai University 17-19. Nov. 2016, Conference book. Electronic ISSN: 2471-9269. INSPEC Accession Number: 16656968. DOI: 10.1109/CINTI.2016.7846421. pp. 295 -298.

[17] Csubák, D. - Szücs, K. - Vörös, P. - Kiss, A. (2016): Big Data Testbed for Network Attack Detection. Acta Polytechnica Hungarica Volume 13 Issue Number 2. DOI: 10.12700/APH.13.2.2016.2.3. pp. 47-57.

[18] Z Rajnai, B. Puskas (2015): Requirements of the Installation of the Critical Informational Infrastructure and its Management, Interdisciplinary Description of Complex Systems 13: (1) pp. 48-56.

[19] Nyikes, Z., Németh, Z. Kerti, A. (2016): "The electronic information security aspects of the administration system," 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI). Timisoara. DOI: 10.1109/SACI.2016.7507395. pp. 327-332.