Műszaki Tudományos Közlemények vol. 9. (2018) 215–218
https://doi.org/10.33894/mtk-2018.09.49
Hungarian: https://doi.org/10.33895/mtk-2018.09.49,
http://eda.eme.ro/handle/10598/30333

PENSION PAYMENT AS A CRITICAL INFRASTRUCTURE

Zsolt Mihály SZABÓ

Óbuda University, Károly Keleti Faculty of Business and Management, Doctoral School on Safety and Security Sciences, Budapest, Hungary, zsolt@tamiyary.hu

Abstract

Today, the state, its organizations and its citizens have become vulnerable to the complexity of complex electronic information systems in the cyberspace of Hungary, without which state operations and the provision and use of different services become unworkable. In addition to the modern economic system, society is not prepared to operate without lost infrastructure, assets or services, so they must clearly be protected especially because the information used and generated in their operation and the data managed represent significant assets.

Keywords*: pension payments, retirement security, information security, IT security, threats and risks.*

1. Introduction

Security is the state in which activities important for the organization can be performed undisturbed. The systems guaranteeing the security of organizational activities must cover all activities affected by organizational strategy [1]. Organizational and IT security strategy guarantee comprehensive and uniform security. The IT security system needs solutions that satisfy security requirements with the lowest, accepted residual risk [2]. The attacks are basically directed to data, which is surrounded by various system elements and handled by processes. Cyber threats threaten data and the processes handling it through a definite chain of system elements [3].

2. Critical infrastructure

The general concept of critical infrastructure can be found on the website of the National Directorate General for Disaster Management, which belongs to the Ministry of the Interior. Critical infrastructure is all the organizations, networks, facilities or facility systems (or parts of these) that create the intellectual and material living conditions of the population of a country, and enable or facilitate the operation of the economy. The destruction of critical infrastructure or a reduction in its services or availability has a negative effect on the existence, living and operating conditions of a given set of users [4]. Based on the above, a possible definition of critical infrastructure for Hungary can be made: a network of connected, interactive (mutually dependent on each other) infrastructure elements, facilities, services, systems and processes which are vital to the operation of the country and have an essential role in maintaining a minimal level of security, economic operation, public health and environment expected by society [5].

Hungary, as a member state, has to adapt the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection to Hungarian law [6]. This means the measures have to be taken which include the directive in the Hungarian legal system. Point f) of the Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities [7] describes which sectors have to be considered as a critical system element. A system element of a tool, facility or system belonging to the defined sectors which is essential for the performing of vital social tasks – especially health care, the personal and property safety of the population, and economic and social public services – and whose in operation would lead to serious consequences as these tasks would not be performed continuously. Section 16b of Ap-

pendix 2 of the above-mentioned law covers the social insurance sector.

The IT systems and records of social insurance are among vitally important systems. Therefore, Government Decree 65/2013. (III. 8.) about the above-mentioned Act CLXVI of 2012 has to be followed [7]. Vitally important IT systems and facilities according to the Government decree are network-like physical or virtual systems, tools and methods of society which are themselves vitally important system elements continuously providing information or ensuring the continuous provision of information, or indispensable for the operation of other identified vitally important system elements.

Risk analysis has to be performed. The threat and risk factors have to be examined concerning the vulnerability of system elements and the consequences of their disturbance or destruction [5]. A possible method can be a CRAMM (CCTA Risk Analysis and Management Method) based methodology [8] [9], adopted by MeH ITB 8. recommendation (IT security methodology manual). It is one of the most widely used methodologies nowadays (see Figure 1.). This method describes the vulnerable points of IT systems and makes recommendations for countermeasures [2].

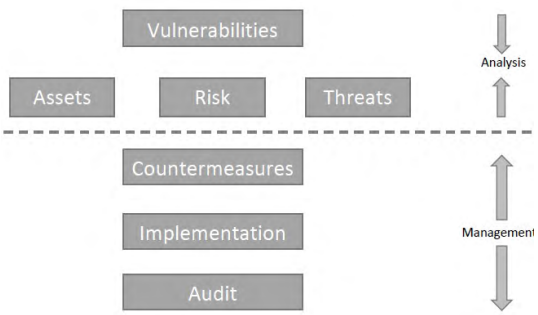

Figure 1. *Risk components, according to CRAMM*

3. Protecting the critical infrastructure

Critical Infrastructure Protection (CIP) is a challenge of the modern age, which got into the limelight worldwide as global terrorism spreads. Infrastructures deemed critical are the ones which enable the basic operation of a society or economy. Protection is especially important nowadays, in the age of 4th generation, or asymmetric warfare (4GW), when almost any interest group can enforce their interests against much larger opponents – typically nation states. The main targets of these attacks are critical infrastructures (CI), especially critical information infrastructures (CII) [10].

The state keeps a record of the data of its citizens with the help of critical infrastructure elements, public administration works using these (not only e-public administration), and the state provides services (not only e-government services) with these. Protecting these is mostly the task of the state, and organizing protection is exclusively the task of the state. All the more so, because the state itself depends on these infrastructures, too. [4]. If a critical infrastructure element stops functioning for any reason, it can practically push the nation-state into chaos and anarchy. For this reason, the state has to focus on performing the tasks accurately and maintaining protection continuously.

Section e) of ACT CLXVI of 2012 defines the protection of a vitally important system element like the following: all activities aimed at ensuring the function, continuous operation and invulnerability of the vitally important system element, and activities aimed at neutralizing or easing the threat, risk or vulnerability [7].

4. Protecting the Pension Payment Directorate, as a vitally important system

Table 1 shows that the pension payment IT system and the connected systems (processes) are especially important (critical) for the operation of the organization, based on damage mode and effect analysis [8] [3].

Act No. L. of 2013. on the Electronic Information. Security of Central and Local Government Agencies prescribes that the IT system of government agencies must be able to monitor and log the critical security events of hardware and software tools vital to the operation of the organization, and automatically handle these events [11]. It is also important that in the IT system and security management of a state organization the implementation of the security policy of the orga-

Table 1. *Examples of high-priority processes*

Name of the Process (System)	System priority level	Time to avert
Pension payment IT system	5 (Critical)	4 hours
Pension payment data query system	5 (Critical)	4 hours
Pension assessment	5(Critical)	4 hours
Filing system	5(Critical)	4 hours

nization can be seen and checked easily [1]. The security management should include as an integral part: network, user, software and firewall management, the content filtering and virus protection of the email system, and other IT systems. Information security requires three basic conditions to be fulfilled simultaneously: confidentiality, integrity and availability. These conditions are related to information [12]. If these conditions are not fulfilled, the IT system can be damaged or the data it handles can be damaged or lost:

– Confidentiality: people other than the those entitled to the information can get access to it;
– Integrity: the information can change while being transferred;
– Availability: the information is not available at the time it is required.

In a larger organization, administrative protection with a hierarchy with organizational and system levels needs to be created.

Designing a defence system does not simply mean constructing a system of devices, but a full process from planning to the realization on the following levels: physical, logical, administrative and human resource defence system [12]. In the case of a larger organisation with extensive IT infrastructure and myriad applications its administrative regulatory background cannot be maintained using one politics and one manual, because in the case these two also cover details, political document (s) and manuals simply fall beyond control and become unmanageable.

Hence administrative defence, as a system, should be given a hierarchical structure partitioned into corporate and system sublevels (see Figure 2.). The most important documents regulating the operation of the organization and which are the most significant normative for IT data security can be divided into two main groups: external documents (security policy, IT security policy, IT security manual, business continuity plan, disaster recovery plan, IT operation regulation, IT development manual, etc.) and internal documents (security policy, IT security policy, IT security manual, business continuity plan, disaster recovery plan, IT operation regulation, IT development manual, etc.)

5. Conclusions

The careful planning of complex IT security determines the IT resource and investment requirements and provides a framework of responsibilities and the focusing of resources on key areas. Only careful planning can ensure that all possibilities of IT can be used to support the organization's goals. Planning must ensure that the solutions to be used can be paid for, are technologically viable, can be properly controlled and can be understood by all people affected.

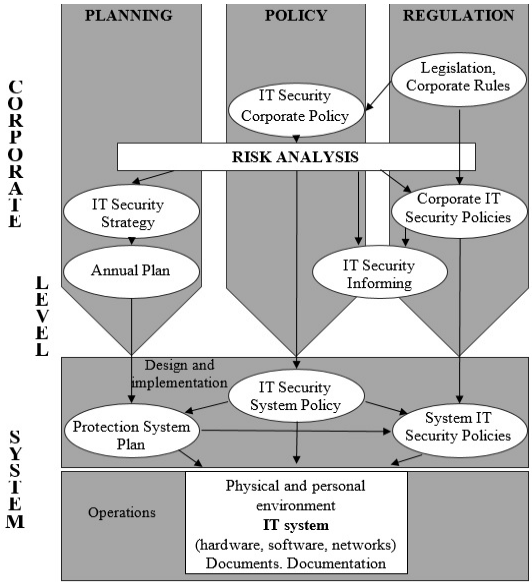

Figure 2. *The process of implementation of IT protection*

References

[1] Michelberger P., Lábodi Cs. : *Vállalati információbiztonság szervezése.* In Vállalkozásfejlesztés a XXI. században II. (Ed.: Nagy I. Z.), Óbuda University 2012. 241-302.

[2] Répás S., Dalicsek I.: *Az információbiztonsági kockázatelemzés módszertani kérdései a kritikus infrastruktúra elemeket üzemeltető szervezetek esetében.* A NKE állam- és közigazgatás-tudományi szakmai folyóirata 4. (2015) 22-33.

[3] Szabó Zs. M.: A *nyugdíjfolyósítás kiberbiztonsági kérdései.* In: VI. IDK2017 (Eds.: Ács K, Bódog F, Mechler M, Mészáros O, Pónusz R), 2017, 507-517.

[4] Katasztrófavédelmi Oktatási Központ (2013): *Létfontosságú Rendszerek és Létesítmények Védelme.* 1-19.

[5] Mógor T., Rajnai Z.: *Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása.* Bolyai Szemle, 33/2. (2014) 43–59.

[6] Directive 2008/114/EC — *Identification and designation of European critical infrastructures and assessment of the need to improve their protection.* European Union Lex. 1-8.

[7] *A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló*

65/2013. (III. 8.) Korm. rendelet (a továbbiakban: Lrtv.). Magyar közlöny 2013. évi 40. sz. 4043-4051.

[8] Szabó Zs. M.: *A nyugdíjfolyósítás információbiztonsági és informatikai biztonsági kérdései.* In: A XXII. Fiatal műszakiak tudományos ülésszak előadásai. Proceedings of the 22th international scientific conference of youngth engineers, Kolozsvár/Cluj, Kolozsvár, Románia, Műszaki Tudományos Közlemények 7. (2017) 363-366. https://eda.eme.ro/handle/10598/29819

[9] Szádeczky T.: Információbiztonsági szabványok. NKE. Budapest, 2014. 1-50.

[10] Sik Z. N.: *A kritikus információs infrastruktúra védelme és a közigazgatás*. Vezetéstudomány 42/3. (2011) 42-47.

[11] *Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény* (a továbbiakban: Ibtv.). Magyar közlöny 2013. évi 68. sz. 50241-50255.

[12] Muha L., Krasznay, Cs.: A*z elektronikus információs endszerek biztonságának menedzselése.* Budapest. NKE Vezető- és Továbbképzési Intézet. 2014, 1-120.