XXII. Fiatal Műszakiak Tudományos Ülésszaka, 2017. Kolozsvár, 363–366. DOI: 10.33895/mtk-2017.07.83
http://hdl.handle.net/10598/29819

A NYUGDÍJFOLYÓSÍTÁS INFORMÁCIÓBIZTONSÁGI ÉS INFORMATIKAI BIZTONSÁGI KÉRDÉSEI

THE PENSION PAYMENTS OF INFORMATION SECURITY AND IT SECURITY QUESTIONS

Szabó Zsolt Mihály

Óbudai Egyetem, Biztonságtudományi Doktori Iskola, H-1081 Magyarország, Budapest, Népszínház utca 8. fszt., +36-1-666-5375, zsolt@tamiyary.hu

Abstract

One of the most important values of economic and social life is information. Information are source of power, basement of efficient operation for organisations, their property and commodity. Security of information is rarely thought of as a problem - but actually series of actions done in order to protect information is netting the everydays of modern life. There are processes that can bring the functioning of an organisation to a critical situation when there are occuring problems if it is not regulated properly and we are not prepared for averting a disaster. This study summarizes the information security systems theoretical background and planning process through a case study is an example of a possible implementation.

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

Összefoglalás

A gazdasági és társadalmi élet egyik legfontosabb értéke az információ. Az információ a szervezetek számára erőforrás, hatékony működés alapja, szervezet vagyona és gyakran termék, áru is. Az információ biztonsága ritkán merül fel bennünk, mint probléma, pedig valójában mindennapjainkat behálózza az információk védelmében tett tevékenységek sorozata. Vannak folyamatok, amelyek kritikus helyzetbe hozhatják a szervezetet működését probléma esetén, ha nem megfelelően szabályozzák a szervezet működését, és hatékonyan nem készül fel a szervezet egy esetleges katasztrófa elhárítására. E tanulmány az informatikai biztonsági rendszer elméleti tervezési folyamatának hátterét foglalja összse és egy esettanulmányon keresztül példát mutat egy lehetséges megvalósításra.

***Kulcsszavak:** nyugdíjfolyósítás, nyugdíjbiztonság, információbiztonság, informatikai biztonság, fenyegetettségek és kockázatok.*

1. Bevezetés

A támadások célja alapvetően az adat, melyet különböző rendszerelemek vesznek körül, folyamatok kezelnek. A fenyegetettségek a rendszerelemek meghatározott láncán keresztül az adatokat és az adatokat kezelő folyamatokat veszélyeztetik. A védelem megvalósítása nem csupán egy eszközrendszer megvalósítását, hanem egy szervezet teljes, azaz fizikai, logikai, adminisztratív és a humánerőforrás védelmi rendszerére vonatkozóan, a tervezéstől a megvalósításig terjedő folyamatát jelenti.

2. Információbiztonság és Informatikai biztonság

Az informatikai biztonság alatt a szervezeti tevékenységek informatikai összetevőinek a célok eléréséhez szükséges megfelelő állapotban tartását értjük [1]. A biztonság a szervezeti működés egyik lényegi eleme egy állami nyugdíjfolyósító esetében a szervezeti kondíciókkal egyenrangú [2]. A szervezeti biztonság komplex fogalom, az egyes részterületek szoros összefüggésben vannak és függenek egymástól. Az alábbi részeket kell figyelembe venni az információbiztonság tervezés során:

- Fizikai biztonság, objektum védelem;
- IT biztonság;
- Ügymenetbiztonság;
- Humán biztonság;
- Papír és hagyományos alapú adatbiztonság.

A fenti részeket figyelembe véve a megvalósítandó védelemnek zártnak, teljes körűnek, a kockázatokkal arányosnak és időben folyamatosan biztosítottnak kell lennie [3]. Egy szervezet informatikai rendszere biztonsági menedzsmentjének kialakításakor annak központosítására, egységes, áttekinthető, számítástechnikai eszközökkel történő támogatására, illetve e rendszer lehető legnagyobb mértékű automatizálására, az emberi tényező lehetőség szerinti kiiktatására kell törekedni. Törvény írja elő, hogy az állami szervek informatikai rendszerének képesnek kell lennie a szervezet működése szempontjából meghatározó hardver– és szoftvereszközök kritikus biztonsági eseményeinek megfigyelésére és naplózására, illetve ezen események automatizált kezelésére. Egy állami szervezet informatikai rendszerének és biztonsági menedzsmentjének kialakításakor a fenti követelményeken túl fontos, hogy a biztonsági rendszerben egyszerűen legyen leképezhető és ellenőrizhető a szervezet biztonságpolitikájának megvalósítása. A biztonsági menedzsmentnek legyen szerves része a hálózat-, felhasználó-, szoftver-, tűzfalmenedzsment, a levelező rendszer tartalomszűrése, vírusvédelme és egyéb más informatikai rendszerek. Az információbiztonság három alapvető követelmény (bizalmassága, sértetlensége, rendelkezésre állás) együttes teljesülése esetén valósítható meg. Ez a három követelmény az információkkal kapcsolatos [4]. Ha ezek a követelmények nem teljesülnek, elveszhet, sérülhet az IT rendszer, illetve az általa kezelt adatok:

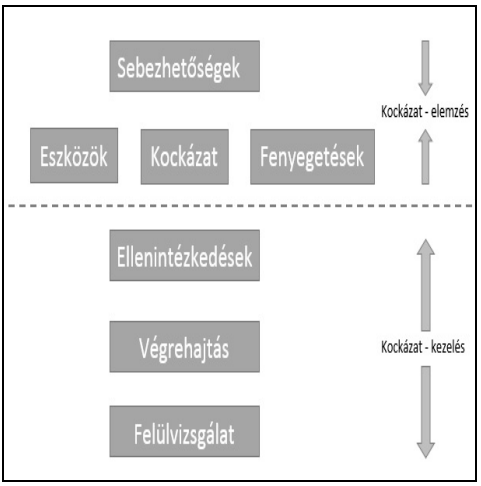
- Bizalmassága: az információt más is megismerheti, mint aki jogosult;
- Sértetlensége: az információ átadása során megváltozhat;
- Rendelkezésre állás funkcionalitása: az információ kellő időben nem hozzáférhető.

Egy nagyobb szervezetnél adminisztratív védelemnek szervezeti és rendszerszintekre tagolt hierarchikus szerkezetét kell kialakítani. A legfontosabb dokumentumok két nagy csoportra oszthatók, melyek egy állami szervezete működését szabályozzák, valamint az elektronikus információs rendszerei adatvédelmére vonatkozó legfontosabb normatívák [5]. A külső dokumentumok (pl. Magyarország Nemzeti Kibervédelmi Stratégiája, Ibtv., Lrtv., Infotv., Mavtv., MeH ITB 8., KIB 25, EU irányelvek, és belső dokumentumok (pl. Biztonságpolitikák, Biztonsági Stratégiák, Biztonsági Szabályzatok) [8]. Minden szervezetnek vannak céljai, amelyeket szervezeti stratégiájukban fogalmaznak meg. A szervezeti stratégiának fontos eleme a biztonsági stratégia. Biztonság alatt azt az állapotot értjük, amelyben a szervezet számára fontos tevékenységek zavartalanul végezhetők. A szervezeti tevékenységek biztonságát szavatoló rendszereknek le kell fednie minden olyan tevékenységet, amelyet a szervezeti stratégia érint. A szervezeti és az informatikai biztonsági stratégia együtt garantálja a biztonság teljeskörűségét és egységes szintjét [6]. Az informatikai

biztonsági rendszernek olyan megoldásokra van szüksége, amelyek a biztonsági követelményeket a lehető legkisebb, már elfogadott maradvány–kockázattal elégítik ki [7].

3. Informatikai biztonság tervezése

Az informatikai biztonság tervezésénél kockázatkezelési módszereket és eszközöket kell alkalmazni [3]. Az emberi tényező, mint más területeken, itt is igen fontos [6]. Kockázatelemzésről nem beszélhetünk korszerű módszerek, eszközök és technikák alkalmazása nélkül.



1. ábra. *Kockázati összetevők a CRAMM módszertan alapján*

A kockázatmenedzsment céltudatos tevékenység, amely kockázatértő szemléletre, kockázatelemzési és kezelési módszerekre, eszközökre és folyamatokra épül [3]. A **1. ábra** mutatja a kockázati összetevőket a CRAMM szerint. A CRAMM (CCTA Risk Analysis and Management Method) alapú módszertan, amely a MeH ITB 8. számú ajánlás (Informatikai biztonsági módszertani kézikönyv) átvett és az egyik legelfogadottabb metodológia napjainkban. Ez a módszer leírja a számítástechnikai rendszerek sebezhető pontjait, és javaslatokat tesz ellenintézkedésekre.

1. táblázat. *Példa a CRAMM alapú mátrixra*

		Szervezeti hatás (kárérték)				
		1	2	3	4	5
Kockázat gyakorisága	1	E	E	E	E	D
	2	E	E	E	D	K
	3	E	E	D	K	K
	4	E	D	K	K	K
	5	D	K	K	K	K

Az **1. táblázat** egy lehetséges példát mutat a CRAMM 5x5-ös mátrixra [7]. Azokba a mezőkbe, melyeknél elfogadhatók (E) a kockázatok, nem kerülnek kidolgozásra új kockázatjavító intézkedések. A döntés szükségességét (D) tartalmazó mezőkben a szervezet működésének megfelelő döntés szükséges a kockázatok további kezeléséről. A kezelendő kockázatot (K) jelölő mezők esetében intézkedési terv kidolgozása szükséges.

4. Esettanulmány

Egy állami nyugdíjfolyósító a szervezeti és IT stratégiájában meghatározott számos céljának elérése érdekében indította el Ügymenet–folytonosság projektjét. A projekt a szervezet szolgáltatásai megbízhatóságának növelését, továbbá folyamatos és zavartalan működését hivatott elősegíteni oly módon, hogy előre felkészült a váratlan, a szervezeti ügymenetet jelentősen befolyásoló események (katasztrófák) kezelésére. Maga a projekt három fő fázisból állt: 1. Általános informatikai biztonsági átvilágítás; 2. Kockázat- és ügymeneti hatáselemzés; 3. Ügymenet-folytonossági Terv (ÜFT) és Informatikai Katasztrófa Elhárítási Terv (IKET) kidolgozása. A szervezeti rendszer nélkülözhetetlen eleme az informatikai rendszer, ezért a projekt teljes körű biztonsági átvilágítással kezdődött. E fázis eredményei egy önálló jelentésben kerültek összefoglalásra. Az Ügymenet-folytonosság projekthez az átvilágításnak leginkább a rendszerek folytonosságával kapcsolatos

eredményei kerültek felhasználásra, melyet az akciótervbe kellett beépíteni. Az ügymenet-folytonosság tervezés alapját egy kockázat- és kárhatás-elemzés teremtette meg, melynek során a szervezet ügymeneti folyamatai és az azokat támogató informatikai rendszerek kerültek áttekintésre és kockázati alapú besorolása. A szervezeti kockázatot annak a potenciálisan okozott kárnak a nagyságával kellett mérni, amely kár a pénzügyi veszteségen túl imidzs veszteség, ügyfelek esetleges elvesztését is magában foglalta. Az információs rendszerek illetve az azokban kezelt adatok kockázati besorolását az integritás, a rendelkezésre állás, a bizalmasság, azok véletlen vagy szándékos megsértéséből adódó kár, ill. kár-hatás alapján kellett végrehajtani. Minden információrendszerre érvényesíteni kellett egy minimális védelmet, amelynek a szervezet által meghatározott fizikai és logikai védelmi eljárásokat, a vírusmentesítő rendszer alkalmazását, a jogosultsági rendszer használatát kellett tartalmaznia. Az egyes információrendszerek kockázati besorolásához kellett rendelni a szervezet számára lehetséges védelmi megoldásokat, a megkívánt helyreállítási időt és rendelkezésre állást.

5. Következtetések

Komplex informatikai biztonsági rendszer tervezésének ma már elengedhetetlen feltétele a kockázat alapú korszerű tervezési módszerek ismerete és alkalmazása.

Mint a tanulmányból kiderül, nagyon sok szempontot kell figyelembe venni, hogy ezt a típusú munkát siker koronázza.

A tervezés minden esetben meglehetősen intézmény specifikus, az adott intézmény szerkezetét, adottságait messzemenően figyelembe kell venni.

Végezetül nem szabad elfelejteni, hogy az informatikai biztonság témájának nagysága és folyamatos fejlődése miatt, elengedhetetlen, hogy ismereteinket folyamatosan frissítsük és aktualizáljuk.

Szakirodalmi hivatkozások

[1] Michelberger, P. (2013): *Vállalatbiztonság*. In Nagy Imre Zoltán (szerk.), Vállalkozásfejlesztés a XXI. században III. Tanulmánykötet, Óbudai Egyetem. 35-52. oldal.

[2] Michelberger, P., Lábodi, Cs. (2012): *Vállalati információbiztonság szervezése*. In Nagy Imre Zoltán (szerk.), Vállalkozásfejlesztés a XXI. században II. Tanulmánykötet, Óbudai Egyetem. 241-302. oldal.

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

[4] Muha, L., Krasznay, Cs. (2014a): *Az elektronikus információs rendszerek biztonságáról vezetőknek.* Budapest. NKE Vezető- és Továbbképzési Intézet. 1-30. oldal.

[5] Muha, L., Krasznay, Cs. (2014b): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest. NKE Vezető- és Továbbképzési Intézet. 1-120. oldal.

[6] 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, pp. 327-332. DOI: 10.1109/SACI.2016.7507395

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

[8] Szádeczky, T. (2014): *Információbiztonsági szabványok.* NKE. Budapest. 1-50. oldal.

[9] Rajnai Zoltán: *A tábori alaphírhálózat vizsgálata*, Nemzetvédelmi Egyetemi közlemények (ISSN: 1417-7323) 2000: (1) pp. 48-57. (2000), Budapest