Műszaki Katonai Közlöny
XXVIII. évfolyam, 2018. 2. szám

Megyeri Lajos[1]

ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGI MENEDZSMENTJE

(SECURITY MANAGEMENT OF ELECTRONIC INFOCOMMUNICATION SYSTEMS)

Jelen publikáció összefoglalja az elektronikus adatfeldolgozás állandó elveit, amelyre valamennyi alapvető jogszabály és helyi szabályozó támaszkodik, függetlenül az aktuális tartalmi változásoktól. Bemutatja a terület működését jelenleg szabályozó hatályos jogszabályok rendszerét, amelyet a jogszabály alkotók a kor kihívásainak megfelelően időszakonként módosítanak, szellemiségükben azonban változatlanok maradnak. A publikáció kitér az informatikai rendszerek tervezése, kialakítása és működtetése során végrehajtandó kockázatelemzések elkészítésének szabályaira, lehetőségeire.

***Kulcsszavak**: biztonság, jogszabály, kockázat, menedzsment, sebezhetőség, fenyegetés*

This publication summarizes the standard principles of electronic data processing, which is based on all basic laws and local regulators, regardless of current content changes. It presents a system of current legislation that regulates the operation of the area, which the legislators periodically modify, according to the challenges of the age, remain unchanged in their spirit. The publication focuses on the rules and possibilities for preparing risk analyzes to be carried out in the design, design and operation of IT

***Kulcsszavak**: security, laws, risk, management, vulnerability, threat*

BEVEZETŐ

Az elektromos energia felhasználásával működő eszközök fejlődése az elmúlt évtizedekben ugrásszerűen felgyorsult. Elektromos áramot használó eszközök vesznek minket körül, minden eddiginél jobban függünk tőlük. Elég csak egy áramszünetre gondolni, szinte megáll az élet, áram hiányában az alapvető infrastruktúrák működésében is zavar állhat, sok területen kényszerűségből szünetel a munkavégzés is. Az elektronikus működésű eszközök tért hódítottak az élet legkülönbözőbb területein. Használatukkal ugrásszerűen felgyorsult az információáramlás, új távlatok nyíltak az adatok feldolgozásának terén is. A számítógép megalkotása majd tömegcikkszerű megjelenése eddig nem létező tudományok fejlődését indította el. Létrejött az informatika fogalomköre, melynek szakkifejezéseit a különböző nyelveken a mai napig nem vagyunk képesek egységesen értelmezni, ami több nemzetet érintő közös munkavégzés során – például NATO informatikai rendszerek – külön megoldandó feladat.

Az információáramlás felgyorsulása, az adatok eddig elképzelhetetlen mennyiségének tárolása, feldolgozása felvetette a biztonság kérdését is. A történelem során mindig is voltak olyan információk, amelyeket óvni, védeni kellett nehogy olyan személy birtokába kerüljön,

[1]Nemzeti Közszolgálati Egyetem, E-mail: megyeri.lajos@uni-nke.hu. ORCID: 0000-0002-3743-1520

aki ártó szándékkal felhasználhatja az információ jogos birtokosával szemben. Amíg az információ csak szóban és írásban létezett, az információbiztonsági intézkedések is kimerültek a nyelv csonkításában illetve papírok fizikai őrzésében. A számítástechnikai eszközök térhódításával, a megnövekedett adatmennyiséggel és eddig nem létező szolgáltatások megjelenésével együtt azonnal megjelent az igény a tevékenységek biztonságossá tételére is. Eleinte szórványosan és ötletszerűen alkalmaztak védelmi rendszabályokat, majd az informatikai rendszerek nemzetközivé válásával szükségessé vált a rendszabályok szabványosítása, egységesítése, amely egy véget nem érő folyamatos tevékenység. Jelen cikkemben az információbiztonsági alapfogalmak tisztázása mellett ennek a nemzetközi szabályrendszernek a magyarországi vetületével kívánok foglalkozni.

1. AZ INFORMÁCIÓBIZTONSÁG ELEMEI

1.1. alapok:

Az információbiztonság az egyik, meglátásom szerint logikus és értelmezhető felosztás szerint a következő területekből áll:

- Személyi biztonság,
- Dokumentum biztonság,
- Adminisztratív biztonság,
- Elektronikus információbiztonság.

A területek alapvetően elhatárolhatóak egymástól, de esetenként átfedést mutatnak. Az elektronikus információbiztonság területén is kell beszélni például emberi, személyi összetevőkről például a szoftveres védelem kialakítása, üzemeltetése terén. Alapelv, hogy információvédelem kialakításánál központi elemként az adat védelméről kell gondoskodni. Ez megvalósulhat eszközök, helyszín fizikai védelmében, személyeknek az adatokhoz való hozzáférésének feltételekhez kötésében, védelmi rendszabályok, szoftverek alkalmazásával. Fontos tehát, hogy meghatározzuk az adat fogalmát.

1.2. információbiztonsági alapfogalmak:

Védelem:

Tevékenység, illetve tevékenységek sorozata, rendszabályok összessége, amely arra irányul, hogy megteremtse, szinten tartsa, vagy fejlessze azt az állapot, amit biztonságnak nevezünk.

A védelem feladatai:

- megelőzés (a fenyegetés hatása bekövetkezésének elkerülése)
- korai figyelmeztetés (valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni.)
- észlelés (a biztonsági esemény bekövetkezésének felismerése)
- reagálás (a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés)
- eseménykezelés (az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és

felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység)[1]

Biztonság:

A rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Tehát a biztonság egy állapot.

- zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.
- teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.
- folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.
- kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.[2]

A biztonság mindig viszonylagos. Teljes biztonság, mint ideális állapot nem létezik. Mindig a kockázatokkal arányos védelemre kell törekedni egyrészt az erőforrások (pl. pénz) hatékony felhasználása érdekében, másfelől azért mert a biztonság növekedése a rendszer hatékonyságának csökkenésével jár együtt. A file ellenőrző, kártékony kódokat szűrő alkalmazások, a munkaállomásokhoz való hozzáférést fizikailag megnehezítő eszközök és eljárások, a kötelező adminisztratív lépések mindenképpen lassítják, akadályozzák a rendszeren történő munkavégzést. Ezért az informatikai rendszer tervezésekor nagy gondot kell fordítani a biztonsági intézkedések kidolgozásánál az alultervezés és túltervezés elkerülésére.

1.3. Az információbiztonság alapelvei:

Szükségesség és arányosság elve: a közérdekű adat nyilvánosságához fűződő jogot minősítéssel korlátozni csak a vonatkozó (2009. évi CLV) törvényben meghatározott feltételek fennállása esetén, a védelemhez szükséges minősítési szinttel és a feltétlenül szükséges ideig lehet.

Szükséges ismeret elve: minősített adatot csak az ismerhet meg, akinek az állami vagy közfeladata ellátásához feltétlenül szükséges.[2]

2013. évi L törvény1§ (8,38,39) pontjai szerint a minősített adatok kezelése során biztosítani kell az alábbiakat:

Bizalmasság: „*az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról*”

Nyílt adatkezelő rendszerekben gyakori a központi adattárolás, ahol egy adott adatbázishoz, (például az alakulathoz érkezett ügyiratok könyvtára) a rendszer valamennyi felhasználója hozzáférhet. Ez gyors adatcserét, hatékony munkavégzést tesz lehetővé. Hátrány lehet, hogy egyes felhasználók nem csak a saját munkájukhoz szükséges információkat ismerik meg.

[2] Nemzetközi viszonylatban ezt nevezik „need to know” elvnek.

Mivel az adatok nem minősítettek, ez nem jelent titoksértést. Az adatbázist frissítő állománynak nagy figyelmet kell fordítania arra, hogy személyiségi jogokat sértő (például egészségügyi, bűnügyi) adatok központi, bárki által elérhető tárolóra ne kerülhessenek mentésre. Jó megoldást jelent a Magyar Honvédségnél bevezetett, úgynevezett „Információ menedzsment rendszer" (IMR) amely nyílt adatokat kezel, de meghatározható, hogy egyes adatokhoz mely személyek férjenek hozzá, és a hozzáférés tényét, tett intézkedéseket, ügy kapcsán készült ügyiratokat az IMR rendszer visszakereshető formában dokumentálja.

Sértetlenség: *„az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható"*

Azt jelenti, hogy a rendszerben kezelt adat a jogosult felhasználó által készítettel megegyezik minden tulajdonságában. Ennek biztosítása az adattároló hardver elemek elérhetőségének korlátozásával, CRC[3] hibadetektálási módszer alkalmazásával vagy például az elektronikus aláírásnál is használt Hash[4] függvény használatával biztosítható.

Rendelkezésre állás: „*biztosítani kell, hogy a szükséges adatok az arra feljogosított személyek számára a megfelelő időben, formában és tartalommal hozzáférhetővé váljanak*"

Ez azt jelenti, hogy a felhasználó az informatikai rendszerben tárolt adataihoz a munkája ellátásához szükséges mértékben bármikor hozzáférhessen. Nyílt informatikai rendszerekben ez viszonylag könnyen kivitelezhető, meghibásodott rendszerelemek, hardver, szoftver frissítése, javítása, pótlása viszonylag egyszerűen, alapvető logisztikai szabályok betartásával megoldható. A minősített adatokat kezelő informatikai rendszer elemeinek javítása vagy cseréje szigorú szabályokkal meghatározott, amelyektől való bármilyen eltérés biztonsági eseményt[5] jelenthet.

2. AZ ADATOKRÓL

2.1. Az adatokról általában:

Adat meghatározása a 2013 évi L törvény[6] szerint*: „az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas*"

[3] CRC :Cyclic Redundancy Code - ciklikus hibajavító kód, amely az átviteli út által okozott hibák detektálására szolgál

[4] Hash függvény – egyirányú titkosító algoritmus, amely biztosíthatja, hogy ha valamely dokumentum elektronikus továbbítás során tartalmában változik, ez a tény azonnal felismerhető legyen.

[5] biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül. 2013 évi L törvény 1. § (1) 9.

[6] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Az elektronikus információvédelem területén adat alatt a mindennapi használat szintjén legtöbbször adatfile értendő. Emellett léteznek folyamatosan működő hálózatok is, melyek folyamatos – például radar adat továbbítás, online adatbázisok – szolgáltatást nyújtanak. Fontosnak tartom az adatkezelés fogalmának meghatározását is, mert ennek alapján lehet a különböző, adatokkal kapcsolatos tevékenységeket szabályozni. Az adatkezelés fogalma a Nemzeti Adatvédelmi és Információszabadság Hatóság szerint:

2.2. *" az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása,* lekérdezése*, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése*"[3]

Szinte azonos definíció található a 94/2009 HM utasításban, amely a Honvédelmi Minisztérium alárendeltségébe tartozó szervezetek felé ad kötelező érvényű iránymutatást.Az adatkezeléssel kapcsolatos alapelvek a civil és a katonai felhasználási területeken némileg eltérőek. Civil viszonylatban a feladatok döntő részét a személyes adatok, a közérdekű és a közérdekből nyilvános adatok kezelése teszi ki. Ezeket az adatokat közösen nyílt adatoknak is nevezhetjük.

A nyílt adatok kezeléséről a 2011. évi CXII. törvény rendelkezik. Meghatározza az adatfajtákat és az adatok kezelésének a rendjét. Az elektronikus információs rendszerek üzemeltetésével kapcsolatos információbiztonsági teendőkről a 41/2015. (VII. 15.) BM rendelet[7] rendelkezik. A rendelet szerint az elektronikus információs rendszereket biztonsági osztályba kell sorolni. A besorolást a rendszerben kezelt adatok és kockázatelemzés alapján a szervezet vezetője hagyja jóvá. Kulcsfontosságú kérdés a rendszerelem funkciója és a kezelt adatok jellege is. Az adatok védelme esetében a kezelt adatok és a rendszer által nyújtott szolgáltatások alapján más –más biztonsági elemet tart elsőrendűnek:

A nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség követelményét emeli ki,a létfontosságú információs rendszerelemek esetében a rendelkezésre állást követeli meg elsődlegesen,a különleges személyes adatokkal kapcsolatban alapvető igényként fogalmazza meg a bizalmasság fenntartását.

Adatkezelés a Magyar Honvédségnél:

A Magyar Honvédségnél, mint a védelmi szféra valamennyi területén kiemelt jelentősége van a bizalmasságnak. Egyszerűen fogalmazva egy adat inkább semmisüljön meg, mint hogy illetéktelen személyek birtokába kerüljön.

A kezelt adatok a bizalmasságuk szempontjából lehetnek:

- nyílt adatok
- minősített adatok

[7] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

Katonai viszonylatban legtöbbször a „nyílt, nem nyilvános" adatkategória jelenik meg, de az információbiztonsággal foglalkozó szakállomány feladatainak jelentős részét a „minősített" adatok kezelése jelenti. A Magyar Honvédségnél a törvényi szabályozás pontosítása céljából az adatok kezeléséről a 94/2009 évi HM utasítás rendelkezik. Az utasítás megszabja, hogy a nem minősített adatokat is biztonsági osztályokba kell sorolni a következők szerint:

alap biztonsági osztályba kell sorolni a nem minősített adatot;

fokozott biztonsági osztályba kell sorolni a nem minősített nagy mennyiségű személyes adatot, a különleges adatot, az üzleti adatot, a címtáradatot az üzemeltetési adatot a magasabb szintű biztonsági követelmények alkalmazása érdekében"

A minősített adatok fokozott védelme alapvető, törvény által megszabott kötelesség. A jogszabály ezen felül a nem minősített adatok két osztályba rendezését határozta meg, melyben a nyílt adatok egy részének is fokozott védelmet kíván biztosítani.

A 3/2012. (I. 13.) HM utasítás[8] pontosította a védelmi intézkedéseket, és előírta, hogy „a biztonsági követelményeket meghatározott védelmi rendszabályokon és kialakított eljárásokon keresztül kell érvényesíteni, amelyeket Elektronikus Információbiztonsági Szabályzat (a továbbiakban: EIBSZ) formájában kell megfogalmazni, jóváhagyatni és alkalmazni"

A Magyar Honvédség nyílt elektronikus információs rendszere a törvény szerint minimum 4. biztonsági osztályba tartozik. Fentiek szerint a jogszabályok sora a nem minősített adatokat feldolgozó informatikai rendszerekkel szemben is elvárásokat támaszt, követelményeket határoz meg, ennek alapján működik például a Magyar Honvédség nyílt, zártcélú informatikai hálózata is. Az EIBSZ az adatok megfelelő bizalmasságának, sértetlenségének és rendelkezésre állását biztosító helyi szabályozást részletesen tartalmazza. A szabályzatot a rendszer valamennyi felhasználójának ismernie kell.

2.3. Minősített adatok kezelése

A 2009. évi CLV. számú, a minősített adat védelméről szóló törvény[9] szerint minősített adatok a következők:

„*a) nemzeti minősített adat:* a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - a megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és

[8] 3/2012. (I. 13.) HM utasítás honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról.

[9] 2009 évi CLV törvény a minősített adat védelméről.
http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0900155.TV (A letöltés dátuma: 2016.04.16)

tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza;

b) külföldi minősített adat: az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza"

A 2009. évi CLV. számú, a minősített adat védelméről szóló törvény részletesen leírja a minősítők körét, a minősítési eljárást, az alkalmazott jelöléseket és a minősített adat biztonságára vonatkozó általános szabályokat. A törvény nagy jelentőségű újdonsága, hogy a nemzeti minősített adatok kezelésére ugyanolyan rendszabályok alkalmazását írja elő, mint a külföldi minősített adatok esetében. A törvény hatályba lépéséig a nemzeti minősített adatok védelmére nem voltak olyan szigorú fizikai biztonsági követelmények előírva, mint például a NATO adatok védelme esetében.

Hazánk NATO csatlakozása után a NATO információbiztonsági követelményeket a C-M(2002)49 direktíva[10] fogalmazta meg. Ennek alapján kezdődött a NATO minősített információk tárolására, kezelésére akkreditált „NATO T irodák" kialakítása nagy anyagi ráfordítással. A NATO csak akkor volt hajlandó minősített információ átadására az új tagország – Magyarország - felé, ha megteremtjük a személyi, fizikai és adminisztratív feltételeket, melyeket valamennyi tagállamtól elvár a szövetség. Az állam kénytelen volt megteremteni a biztosítani a körülményeket, amelyek azonban csak a NATO minősített adatokra vonatkoztak. Saját nemzeti minősített adatainkat a régebbi előírások szerinti, jóval szerényebb védelmet biztosító feltételek szerint kezelhettük.

A 2009. évi CLV. számú törvény megszüntette ezt a kettősséget és a nemzeti adatok védelmére is a külföldi (lásd NATO) védelmi rendszabályokat léptette életbe. Ez a módosítás rövid távon sok gondot okozott a döntéshozó és végrehajtó állománynak egyaránt. A nagy fizikai védelmet nyújtó védelmi rendszer kiépítése költséges. A végrehajtási utasításokban több évig halasztották a fizikai védelem kiépítésének végső határidejét, hogy a honvédség költségvetéséből megteremthessék a törvény által előírt, elsősorban fizikai biztonsági feltételeket. A törvénynél részletesebb szabályozást tartalmaz a minősített adat elektronikus biztonságának, valamint hatósági felügyeletének részletes szabályairól szóló 161/2010 Kormányrendelet.A minősített adatok kezelésénél valamennyi jogszabály előtérbe helyezi a kockázatok felmérésének és kezelésének szükségességét.

3. KOCKÁZATKEZELÉS

3.1. Kockázatkezelésről általánosan

A mai sokszorosan összetett világban, a tudományágak specializálódása révén a kockázatkezelésnek komoly ismeretanyaga gyűlt össze az élet különböző területein.

[10] Security within the North Atlantic Treaty Organisation (NATO). C-M(2002)49. North Atlantic Council, 2002.

A kockázatok teljes kizárása, teljes biztonság állapota sajnos sohasem érhető el. Minden élőlény, eszköz, rendszer, társadalom sebezhető. A biztonság megteremtésére nem állhat rendelkezésre végtelen idő, pénz, munkaerő. Szükség van az erőforrások ésszerű felhasználására, ebben nyújt segítséget a kockázatok feltárása, elemzése.

A számítástechnikai eszközök gyors fejlődése egyre növekvő méretű informatikai hálózatok kialakulásához vezetett, (pl. Internet). Az informatikai hálózatok kezdetben helyi hálózatban, egymástól függetlenül alakultak ki és fejlődtek. Egy bizonyos szintet elérve, az összekapcsolhatóság érdekében az informatikai hálózatok tervezői kénytelenek voltak közös eljárásrendeket kialakítani. A rendszerek méretének és bonyolultságának a növekedésével egyre nőtt a rendszerelemek sebezhetősége is. Kialakultak szabványrendszerek, melyekben különböző módon, de a kezdetektől fogva megjelent a kockázatkezelés szükségessége.

A várható hatás tekintetében a kockázatok köre két nagy csoportra bontható. Az első csoportba az úgynevezett egyszerű (tiszta, pure) kockázatok tartoznak, melyek esetében a lehetséges kimenetelek az alábbiak lehetnek: (a) kár, veszteség következik be,(b) vagy nem következik be semmilyen változás. Ezzel szemben összetett (speculative) kockázatról beszélünk akkor, ha a vizsgált kockázathoz háromféle kimenetel tartozhat: (a) kár, veszteség következik be; (b) nem történik változás;(c) nyereség, gyarapodás az eredmény.[4]

Az informatikai rendszerek kockázatai véleményem szerint az úgynevezett egyszerű kockázat kategóriába tartoznak, nem várható nyereség reményében kockáztatunk, „csak" a rendszerek folyamatos működését fenyegető kockázatokat kell kezelnünk. Ezzel szemben a tőzsdei befektetésben például összetett kockázatvállalásról beszélhetünk, amikor az bróker eldönti, hogy milyen részvényt vásárol és milyet ad el. Különböző részvényeknek más-más a megtérülési rátája – haszna, de eltérő mértékű a vállalt kockázat is. A bróker átgondolhatja, mekkora kockázatot vállal milyen haszon reményében.

Az informatikai rendszerek esetében a nagyobb kockázatvállalás, kevesebb biztonsági elem használata rövid távon olcsóbbá teheti a kivitelezést. Mégis szükséges a védelmi rendszerünket kockázat elemzés alapján arányos védelemmel kialakítani, mert ezzel csökkenthetjük a releváns fenyegetések bekövetkezésének esélyét. Sajnos nehéz a tulajdonost, döntéshozót rábírni arra, hogy anyagi erőforrásokat fordítson a biztonságra, mert az ebből fakadó „elmaradt kár" nehezen mutatható ki mindaddig, amíg valós biztonsági esemény kapcsán veszteség nem éri a tulajdonost.

3.2. Állami és önkormányzati szervek kockázatkezelése

A költségvetési szervek gazdasági tevékenységével kapcsolatban a „Folyamatba épített előzetes, utólagos és vezetői ellenőrzés" rendszerét (a továbbiakban FEUVE) 2011. évi CXCV. törvény és végrehajtásáról szóló 368/2011. (XII. 31.) kormányrendelet, illetve a költségvetési szervek belső kontrollrendszeréről és belső ellenőrzéséről szóló 187/2016. (VII. 13.) Korm. rendelet határozza meg. Ez utóbbi szerint*:" integrált kockázatkezelési rendszer: olyan folyamatalapú kockázatkezelési rendszer, amely a szervezet minden tevékenységére kiterjed, egységes módszertan és eljárások alkalmazásával, a szervezet célkitűzéseinek és értékeinek figyelembevételével biztosítja a szervezet kockázatainak teljes körű azonosítását, azok meghatározott kritériumok szerinti értékelését, valamint a kockázatok kezelésére*

vonatkozó intézkedési terv elkészítését és az abban foglaltak nyomon követését;" Kockázatelemzés: objektív módszer az ellenőrizendő területek kiválasztására, mely meghatározza a költségvetési szerv tevékenységében és belső kontrollrendszerében rejlő kockázatokat"[5]

Tehát az a legfontosabb, hogy a szervezet minden tevékenységi körében értelmezze és értékelje a kockázatokat. A tevékenységek szabályos működését beosztás, munkakör szerinti, személyes felelősséghez köti. Az elemzést (FEUVE) minden naptári évben el kell végezni, a felelős személyekkel meg kell ismertetni és a szervezet vezetőjének kell jóváhagynia.

A FEUVE rendszere a következő kockázatok kezelését határozza meg:

- Külső kockázatok, melyeknek csökkentésére alig van lehetőségünk:
- Infrastrukturális: Az infrastruktúra elégtelensége vagy hibája akadályozhatja a normális működést.
- Gazdasági: Az infláció negatív hatással lehet a költségvetési előirányzatokra.
- Jogi és szabályozási: A jogszabályok és egyéb szabályok korlátozhatják a kívánt tevékenységek terjedelmét. A szabályozások nem megfelelő megkötéseket tartalmazhatnak.
- Politikai: Egy kormányváltás megváltoztathatja a kitűzött célokat, a célok prioritását. Piaci Szállítói probléma negatív hatással lehet a tervekre.
- Elemi csapások: Tűz, árvíz vagy egyéb elemi csapások hatással lehetnek a kívánt tevékenység elvégzésének képességére.
- Pénzügyi kockázatok
- Költségvetési: A kívánt tevékenység ellátására nem elég a rendelkezésre álló forrás. A források elosztása nem befolyásolható közvetlenül
- Pénzügyi: Eszközvesztés. A források nem elegendőek a kívánt megelőző intézkedésre. Tevékenységi kockázatok
- Működés-stratégiai: Nem megfelelő stratégia követése. A stratégia elégtelen vagy pontatlan információra épül. Működési Elérhetetlen/megoldhatatlan célkitűzések. A célok csak részben valósulnak meg.
- Információs: A döntéshozatalhoz nem megfelelő információ a szükségesnél kevesebb ismeretre alapozott döntést eredményez.
- Hírnév: A nyilvánosságban esetlegesen kialakult rossz hírnév negatív hatást fejthet ki.
- Technológiai: A hatékonyság megtartása érdekében a technológia fejlesztésének/lecserélésének igénye. A technológiai üzemzavar megbéníthatja a működést.
- Projekt: A megfelelő előzetes kockázatelemzés, hatástanulmány nélkül elké- szülő projekt-tervezet. A projektek nem teljesülnek a költségvetési vagy funkcionális határidőre.
- Újítás: Elmulasztott újítási lehetőségek. Új megközelítés alkalmazása a kockázatok megfelelő elemzése nélkül.

Emberi erőforrás kockázatok

- Személyzeti: A hatékony működést korlátozza, vagy teljesen ellehetetleníti a szükséges számú, megfelelő képesítésű személyi állomány hiánya.

- Egészség és biztonsági: Ha az alkalmazottak jó közérzetének igénye elkerüli a figyelmet, a munkatársak nem tudják teljesíteni feladataikat.

Mindezeken felül érvényes a 2013 évi L törvény az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény, amely kifejezetten foglalkozik az elektronikus információbiztonsággal kapcsolatos kockázatkezeléssel.

3.3. Létfontosságú rendszerek, kritikus infrastruktúrák:

A „65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról” szükségesnek tartja a létfontosságú rendszerek és létesítmények védelmével kapcsolatban a kockázatelemzés szükségességét. A kockázatelemzés fogalmát az alábbiak szerint határozza meg:

„kockázatelemzés:fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából;”[6]

A fogalom véleményem szerint nem letisztult, a kockázati tényezők vizsgálatára nem ad egyértelmű iránymutatást. A jogszabály nem fogalmaz meg kötelező érvényű szabályokat a kockázatelemzés végrehajtásának módszerére, de a kockázatok azonosításának és értékelésének a módját részletesen leírja:

A jogszabály a rendszerelemet fenyegető kockázati lista készítését írja elő valamennyi rendszerelemre vonatkozóan majd a kockázatok valószínűsíthető okainak feltárását határozza meg a várható negatív hatás meghatározásával együtt. A kockázati lista elkészítésénél gondosan kell eljárni, a rendszerelemek sebezhetőségének alapos figyelembevételével. Paráda I. „Webkamera hack – penetration teszt.”[7] című cikkében rámutat például, hogy a webkamerák üzemeltetése során milyen módszerekkel lehet a rendszerbe illetéktelenül behatolni és információhoz jutni. Az általa leírt eljárásrend megmutatja, milyen fontos a megfelelő szoftverek használata, különös tekintettel az alkalmazott beállításokra.

A jogszabály a kockázatok értékelését írja elő, majd a kockázatok kezelését a kockázati szint függvényében bár a jogszabály a kockázatelemzés módját nem határozza meg.

A kockázatelemzés eredményét úgynevezett azonosítási jelentésben meg kell jeleníteni. Az üzemeltető a kockázatelemzés típusától függően a kockázati szinteknek megfelelően foganatosít biztonsági intézkedéseket a rendszerelem biztonsága érdekében. A létfontosságú rendszerelemek Üzemeltetői biztonsági tervében szerepeltetni kell a főbb fenyegetettségek elemzését és az egyes elemek sebezhetőségén, valamint a lehetséges hatásokon alapuló kockázatelemzést. A jogszabály a részleteket nem határozza meg, de véleményem szerint célszerű egy átfogó kockázatelemzés egyik részterületének tekinteni a rendszerelem információs infrastruktúrájának vizsgálatát és a részterület elemzését a szakmában járatos lehetőleg független szakemberekkel célszerű elvégeztetni.

Összességében megállapítható, hogy a létfontosságú rendszerelemek vonatkozásában a kockázatelemzés megléte kötelező, tartalmi, módszertani megkötéseket azonban a jogszabály nem tartalmaz.

A jogszabály megemlíti a honvédelmi létfontosságú rendszerelem fogalmát is, a fent leírt szabályok betartása ezen rendszerelemekre is vonatkoznak.

3.4. Kockázatkezelési módszerek:

A kockázatkezelés elméleti formái véleményem szerint az alábbi csoportosításban tágyalhatóak:

Kockázatkerülés

Bizonyos károk, veszteségek esélyének a teljes kiküszöbölését jelenti. Jelentheti azt, hogy a szervezet az elemzés alapjául szolgáló tevékenységével a kockázatok növekedése miatt felhagy. A CRAMM tipusú kockázatelemzésben meghatároznak egy szintet, amelynél magasabb szintre kockázat nem kerülhet. Ha egy kockázatot semmilyen módszerrel nem lehet az adott szint alá csökkenteni, az informatikai rendszernek azt a részét, amely az adott kockázattal jár, az adott helyszínen meg kell szüntetni. Általános, minden területre kiterjedő kockázatkerülés nem lehetséges, mert ez a vizsgált rendszer működésképtelenségét jelentené. Egyes szolgáltatások megszüntetése a túlzottan magas kockázat miatt lehetséges.

Kockázatok csökkentése

Ez az elv jelenti a valódi kockázatkezelést, mert itt a kockázat csökkentésére a szervezet saját szervezési stratégiáját és hardver – szoftver eszközeit használjak fel. Az eljárások, melyek ebbe a csoportba tartoznak, három részre oszthatók.

A kármegelőző (pre-loss) elvek biztosítják azt, hogy a szervezet gazdaságosan, a jogszabályoknak megfelelően működjön. Nem lehet cél a teljes mértékű biztonság, hiszen ez gyakorlatilag lehetetlen. Ebbe a csoportba tartozik az épületek, gépek, járművek, berendezések szabályszerű, rendszeres karbantartása, redundáns eszközök, hálózatok használata, átgondolt szakszerű üzemeltetés-informatikai rendszerek védelmi rendszere, tűzfal, kártékony programok elleni védelem, szabályzatok, utasítások kidolgozása, a menedzsment és a felhasználói állomány kiválasztása, felkészítése, továbbképzése.

A kárenyhítő (pro-loss) kockázatkezelés nem a károk bekövetkezésének megakadályozásával foglalkozik, mert itt a bekövetkezett károk hatásának enyhítése a cél. Alapvető követelmény a rendszer visszaállítása a lehető legrövidebb időn belül a lehető legkisebb adatveszteséggel a lehető legkisebb anyagi és humán erőforrás ráfordítással. Fontos, hogy a szervezet alaprendeltetésből adódó működőképessége folyamatosan fennmaradjon.

A harmadik kategóriába tartoznak azok a vállalt kockázatok, melyek nem igényelnek semmiféle intézkedést. Ennél a stratégiai részterületnél a passzivitás az irányadó. Ezek olyan kockázatok melyek elhanyagolhatóak, elenyészőek, de mégsem illenek bele az előbbi két csoportba. Egyes terminológiákban ezt maradvány kockázatnak nevezik, melyet a szervezet vezetőjének írásban el kell fogadnia.

Kockázatmegosztás, kockázatáthárítás

Több szervezet együttműködése esetén, kiszervezett szolgáltatások igénybe vétele esetén mindenképpen megoszlik a vállalt kockázat. Létrejöhet szerződéses alapon akár biztosítótársaságok közreműködésével is. A partnerek lehetnek állami szervezetek, hatóságok,

üzleti partnerek, befektetők, pénzintézetek is. Az üzleti szerződések feltételeinek megfelelő alakítása lehet az egyik módja a kockázat áthárításának. A szerződés megkötésekor mérlegelni kell a kockázatokat és azok elosztását a szerződő felek között. A biztosítás is áthárító, kockázatmegosztó jellegű. [8]

Nemzetközi szabvány:

Az ISO/IEC 27005: 2011 [9] szabvány foglalkozik az információbiztonsági kockázatelemzés egységesítésével nemzetközi szinten.

Az ISO / IEC 27005: 2011 segíti a felhasználókat az információbiztonsági irányítási rendszer szabványának (ISO / IEC 27001) kockázatkezelési megközelítésen alapuló végrehajtásában. Meghatározza az információbiztonsági kockázatkezelési folyamat lépéseit a következők szerint:

- Kontextus létrehozása
- Kockázatelemzés
- Kockázat kezelés
- Kockázat elfogadás
- Kockázati kommunikáció
- Kockázatfigyelés és felülvizsgálat

A kockázatkezelés gyakorlati formái a következők lehetnek:

A kockázat elemzésre, jelentés elkészítésére jogszabályi előírás van. Ennek eredményeként sok vállalkozás foglalkozik ennek elkészítésével. Kifejlesztettek szoftvereket is, amelyek megkönnyíthetik a kockázatelemzést végrehajtók munkáját. A közszférában és például a Magyar Honvédségnél is a szervezet munkatársai készítik az elemzéseket úgy, hogy szerencsés esetben előzetes felkészítésen vettek részt a végrehajtás lehetséges módjait illetően. A lehetőségek sokaságából kiemeltem két egymástól erősen különböző módszert. Ezeken kívül még számos más típus létezik. A választásom azért esett az alábbiakban bemutatottakra, mert a CRAMM módszer információbiztonsági szervezetek ajánlása alapján talán a legalkalmasabb módszer, a másik típusú elemzést pedig szintén használják a közszférában, de nem információbiztonsági szakterületen.

Gordon-Loeb Model:

2002-ben Gordon és Loeb [10] egy egyszerű és nagyon általános modellt javasolt a sebezhetőség csökkenésének értékelésére. A Gordon-Loeb / gȯr-dən lōb / modell egy matematikai gazdasági modell, amely elemzi az optimális befektetési szintet az információbiztonságban. A modell bonyolult matematikai számítások segítségével megmutatja, hogy egy információs rendszer kiberbiztonsági tevékenységeire fordítandó összeg növelése egy bizonyos határon túl nem költséghatékony az információs rendszer sebezhetőségének kezelésére. Meghatározza azt a pontot, ameddig érdemes elmenni anyagi erőforrások ráfordításával az információbiztonság növelése érdekében. A modell kifejezetten a megtérülési szempontokat veszi figyelembe.

Hibafa elemzés (FTA):

Katasztrófavédelemhez kapcsolódó rendszerek, veszélyes üzemek biztonsági elemzéséhez használják. A módszer egyik alapvető előnye az, hogy olyan meghibásodási lehetőségek szisztematikus és logikus feltárására és feldolgozására alkalmas, amelyek súlyos baleset kialakulásához vezethetnek. Ez a fajta feldolgozás azt igényli, hogy az elemzést végző teljes mértékben ismerje és értse az üzem vagy a rendszer működését, valamint a berendezések különböző meghibásodásainak módjait.

A hibafa elemzés az eseményeket a súlyos balesethez vezető berendezés meghibásodásokra és az emberi tévedésekre bontja fel. A módszer ezért egy fordítva gondolkodási technika, azaz az elemző a súlyos balesetből, vagy a nemkívánatos esetekből indul ki. Ezeket el kell kerülni, és meg kell határozni az eseményt közvetlenül kiváltó okokat. Sorba vesszük a közvetlen kiváltó okokat, továbbá mindig megállapítjuk az eseményhez vezető alapvető okokat. A hibafa olyan ábra, amely szemlélteti ezeket az alapvető okokat, továbbá az okok és a baleset közötti összefüggéseket. Az ábrán „ÉS" „VAGY" kapuk jelölésével mutatják be, hogy bizonyos események együttes előfordulása eredményezhet negatív kimenetelt, ami további negatív eredményeket hozhat, ami végül a „csúcsesemény" mint lehető legrosszabb következmény megvalósulásáig vezet.

A hibafa elemzés eredménye azoknak a berendezés-hibák és az emberi hibák kombinációjának felsorolása, amelyek elegendőek egy súlyos baleset kiváltásához. A meghibásodásoknak ezeket a kombinációit minimális hibaesemény kombinációnak nevezik. Mindegyik minimális hibaesemény kombináció a berendezés- és az emberi hibák olyan legkisebb halmaza, amely elegendő egy súlyos baleset előidézéséhez, ha ezek a minimális hibaesemény kombinációban levő meghibásodások együtt, és egyszerre jelentkeznek.[11]

CRAMM[11] típusú kockázatelemzés:

A CCTA[12] által kidolgozott módszertan elsősorban az információs rendszerek kockázatkezelésére alkalmas. A kockázatelemzés gyakorlati végrehajtása három fő feladatcsoportra bontható, melyek további részfeladatokból állnak.

Az első feladatcsoportban az alapvető szempontok kerülnek megállapításra:

- Meghatározásra kerül a kockázatelemzés hatóköre.
- Azonosításra és értékelésre kerülnek a rendszer vagyonelemei.

A második feladatcsoportban megtörténik a kockázat értékelése a javasolt biztonsági követelmények szerint.

- A rendszerre potenciális veszélyt jelentő fenyegetések azonosítása, a fenyegetések típusának és fokának a megállapítása.
- A rendszer sérülékenységeinek a feltárása, melyeken keresztül a fenyegetés érvényre jutva biztonsági eseményhez vezethet.
- A fenyegetés illetve a sérülékenységi halmaz összevetése, és kockázati értékek kiszámítása szorzással, összeadással, súlyozással, a kockázat értékelő döntése szerint.

[11] CRAMM - ***C****entral Computer and Telecommunation Agency* ***R****isk* ***A****nalysis and* ***M****anagement* ***M****ethod*
[12] Central Computer and Telecommunation Agency (Egyesült Királyság)

A harmadik feladatcsoportban megállapításra kerül, milyen szint feletti kockázatokat kell kezelni, illetve megállapítják azon ellenintézkedéseket, melyekkel az adott kockázatok szintjét az elviselhetőség szintje alá lehet csökkenteni.

Az információs rendszerekben a védendő legfőbb érték az adat, amelynek a feldolgozására a rendszert létrehozták. Az adat védendő alaptulajdonságai az adat bizalmassága, sértetlensége és rendelkezésre állása[13] valamint hálózati adattovábbítás esetén a továbbítás letagadhatatlansága és hitelessége. A kockázatelemzés értékelését mindig a fenti tulajdonságok megőrzése szempontjából kell végezni. A tárolt adatok jellegétől illetve a rendszer által nyújtott szolgáltatások jellegétől függ, hogy melyik a leginkább védendő tulajdonság. A védelmi szférában általában a bizalmasság a legfontosabb. Egy oktatási célból létrehozott adatbázis vagy egy elektronikus menetrend (ELVIRA) adattár esetén a sértetlenség és hitelesség a legfontosabb, bizalmasságot nem is kell biztosítani, hiszen ezek az információk bárki számára elérhetőek kell, hogy legyenek.

4. ÖSSZEFOGLALÁS

Jelen cikkemben összefoglaltam az elektronikus adatfeldolgozás állandó elveit, bemutattam a terület működését jelenleg szabályozó hatályos jogszabályok főbb elemeit. Kitértem az informatikai rendszerek tervezése, kialakítása és működtetése során végrehajtandó kockázatelemzések lehetőségeire, alapvető jellemzőikre, elkészítésének szabályaira, Bemutattam, hogy különböző szakterületek más-más eljárást alkalmaznak a kockázataik elemzésére. A kockázatelemzések elkészítésére szakterületenként különböző szoftvereket is alkalmaznak. Ezek alkalmazása megkönnyíti a munkát, különösen nagy kiterjedésű bonyolult rendszerek esetén, de szem előtt kell tartani, hogy a program nem helyettesítheti az embert, a kockázatelemzésre a vizsgálandó rendszer valamennyi részterületéről szakembereket kell bevonni.

Megállapítottam, hogy bár az információs rendszerek esetében is léteznek szabványok és ajánlások,ISO/IEC 2700:2011) de egyik ajánlás sem határozza meg a kockázatkezelés pontos módját.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény előírja az informatikai rendszerek biztonsági osztályba illetve szintbe sorolását, kockázatelemzés alapján. Új informatikai rendszerek tervezésénél, különösen ha minősített adatokat is kell kezelni, kezdeti kockázatelemzést kell végrehajtani. A kockázatelemzés végrehajtása meghatározott esetekben, jogszabályban előírt kötelezettség.

A kockázatelemzési módszerek közül információs rendszerek esetében véleményem szerint a CRAMM típusú kockázatelemzés a leghatékonyabban alkalmazható. Kifejezetten elektronikai rendszerek elemzéséhez fejlesztették ki. Hasznosak lehetnek a vagyontárgyak, fenyegetések, sebezhetőségek előre elkészített listái, melyeket előre, rendszerre tipizálva el lehet készíteni. Az elemzés számításai logikusak, nem igényelnek kiemelkedő matematikai képességeket, mint a Gordon-Loeb modell, ami azért lehet fontos, mert egy új vagy kiterjedt informatikai

[13] Fogalmak meghatározása a 2013 évi L törvény 1. § (1)

hálózat esetében sok telepítési helyen kell egyszerre elkészíteni az elemzést, és a szakemberek képességei és ismeretei sem egyformák.

FELHASZNÁLT IRODALOM

[1] 2013. évi L törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1. § (46)

[2] 2013. évi L törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1. § (21,31,44,48)

[3] https://www.naih.hu/adatvedelmi-szotar.html Letöltés ideje:2017. október 27.

[4] PÁLINKÁS P.: Kockázatkezelési eljárások alkalmazása az európai unió mezőgazdaságában doktori (phd) értekezés [Szent István egyetem, Gödöllő 2011 10. oldal.] gazdálkodás és szervezéstudományok doktori iskola

[5] 187/2016. (VII. 13.) Korm. rendelet 2. § l.

[6] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról, **1. §** 2.

[7] PARÁDA I.:WEBKAMERA HACK – PENETRATION TESZT *HADMÉRNÖK* XII**:** (különszám) *pp. 204-216.* (2017) Katonai Műszaki kutatások aktuális kérdései. Budapest, Magyarország: 2017.05.11 (ISBN 1788-1919)

[8] SÁNDOR B.: A Kockázatkezelés Jelentősége Budapesti Gazdasági Főiskola Budapest, 2011. http://elib.kkf.hu/edip/D_15929.pdf (Letöltés időpontja: 2017.10.20.)

[9] https://www.iso.org/news/2011/08/Ref1451.html (Letöltés időpontja: 2017.10.21.)

[10] LAWRENCE A. G. és M. LOEB a Marylandi egyetem professzorai (https://www.umd.edu/)

[11] kok.katasztrofavedelem.hu/letoltes/document/document_181.doc. (Letöltés időpontja: 2017.10.20.)