ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Kockázatértékelés, kockázatmenedzsment

Dr. László Gábor

Nemzeti Közszolgálati Egyetem

Budapest, 2014

Tartalomjegyzék

Ábrák jegyzéke 4

Táblázatok jegyzéke 4

Mellékletek jegyzéke 4

Bevezetés 1

1 Fogalmi keretrendszer 3

1.1 Az információbiztonság alappillérei 4

1.2 Védelemi intézkedések, szintek 6

2 A kockázatértékelés, a kockázatelemzés, és a kockázat-menedzsment kapcsolata . 7

3 Kockázatértékelés 8

4 Kockázatelemzés 10

4.1 A kockázatok azonosítása, veszélyforrások listájának összeállítása 11

4.1.1 Vagyontárgyak azonosítása, erőforrás lista 13

4.1.2 A sérülékenységek – sebezhetőségek 13

4.1.3 Veszélyforrások csoportosítása 14

4.1.4 Veszélyforrások feltárásának módszerei 15

4.2 A bekövetkezési valószínűség megállapítása 16

4.3 Lehetséges károk és értékük meghatározása 17

4.4 Kockázati tényezők származtatása 19

4.5 Kockázatok kezelése, védelemi intézkedések számbavétele 20

5 Üzletmenet-folytonosság és katasztrófatervezés 24

5.1 Üzletmenet-folytonossági terv (BCP) 24

5.2 Katasztrófa-elhárítási terv (DRP) 25

5.3 Incidenskezelési terv (IRP) 25

Összefoglalás 26

Felhasznált irodalom 27

Mellékletek 29

Ábrák jegyzéke

1. ábra IT kockázatok elhelyezkedése a kockázatok hierarchiájában 9
2. ábra Védelmi intézkedések, fenyegetettségek 12

Táblázatok jegyzéke

1. táblázat Kockázatelemzési táblázat 15
2. táblázat Bekövetkezési valószínűségek 16
3. táblázat Kockázatelemzési táblázat – bekövetkezési valószínűségek 16
4. táblázat Kárkategóriák meghatározása 18
5. táblázat Kárérték táblázat 18
6. táblázat Kockázatelemzési táblázat – kár CIA kategóriáknak megfelelően 19
7. táblázat Kockázati szorzótábla 20
8. táblázat Kockázatelemzési táblázat – Kockázat 20
9. táblázat PreDeCo-CIA mátrix 22
10. táblázat Védelmi intézkedések – példa vírustámadás esetén 23
11. táblázat Kitöltött kockázatelemzési táblázat 23

Mellékletek jegyzéke

1. melléklet ENISA kockázatmenedzsment/ kockázatelemzés módszertanok i
2. melléklet ENISA kockázatmenedzsment/ kockázatelemzés eszközök ii
3. melléklet Lehetséges kárértékek iv

Bevezetés

Az elmúlt évtizedekben az informatika megkerülhetetlenül beépült az üzleti szervezetek, kormányzatok és az emberek mindennapjaiba. Erre jól rávilágít Nicholas G. Carr 2003-as cikke, amely széleskörű visszhangot és vitát váltott ki ellenzői, és támogatói között. Carr nézete szerint az IT beépült a cégek mindennapjaiba, tömegtermékké vált. Nem jelent többé versenyelőnyt, de szükséges a versenyben maradáshoz. (Carr, 2003)

Újabb technológiák és üzleti modellek nyernek teret maguknak, amelyek sokszor megkönnyítik a munkát, azonban újabb biztonsági kihívásokat is jelentenek – gondoljunk a felhő alapú szolgáltatásokra, vagy a BYOD[1] jelenség elterjedésére – továbbá ezeket a folyamatosan hálózatra kapcsolt eszközöket a kiberbűnözés is fenyegeti. A kiberbűnözés is átalakult az elmúlt években, elsősorban a haszonszerzés, valamint a károkozás vált az elsődleges céllá. A Secunia 2013 végén megjelent biztonsági jelentése szerint a kormányzatok voltak a kibertámadások elsődleges célpontjai. A kormányzati szektorban jelentős mennyiségű bizalmas, titkos gazdasági, társadalmi és katonai adatokat, információkat tárolnak és kezelnek. Ezen adatok védelme prioritást élvez, így világszerte a kormányzati szektor fordítja a legtöbbet az IT biztonságra. A jelentés alapján a fenyegetettséget alapvetően a rendszerek és programok sérülékenységei, és ezen sérülékenységek nem megfelelő kezelése jelentette. Egy súlyos sérülékenység támadók általi kihasználása a rendszer kompromittálódásához vezethet, ezáltal akár súlyos szocio-gazdasági következményekkel is járhat.

Magyarországon a 2013. évi L. törvény rendelkezik az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban Ibtv.). A törvény megfogalmazza az alapvető elektronikus információbiztonsági követelményeket, továbbá az elektronikus információs rendszerek biztonsági osztályba, a szervezetek biztonsági szintekbe sorolásának alapelveit, a kapcsolódó feladatokat, felelősöket, intézményeket, hatóságokat.

Az IT biztonság kezelésének problémája túlmutat az informatikai rendszereken; az egész szervezet felépítését, üzletmenetét, folyamatait érintő kérdésről van szó. Az elektronikus információs rendszer biztonságáért felelős személy egyik legfontosabb feladata, hogy a szervezeten belül kialakítsa és ellenőrizze azokat az információbiztonsági szabályokat, amelyek az informatikai rendszerekkel kapcsolatba lépőkre vonatkoznak. Ennek megfelelően

[1] Bring Your Own Device – hozd a saját eszközödet

az összeférhetetlenség elkerülése érdekében ez a felelős személy nem lehet sem az IT vezető, sem a rendszergazda.

A különböző tevékenységeket végző szervezeteknek különböző típusú kockázatokkal kell szembenézniük. Minden szervezetnek egyedi IT kockázati profilja van a használt rendszerek és kapcsolódások függvényében, így csak általános iránymutatást lehet megfogalmazni, amelyet az adott szervezet sajátosságainak figyelembevételével kell implementálni a kockázatfelméréstől kezdődően, a jogszabályi előírások figyelembevételével.

A kockázatelemzést és módszertant az egyik törvényileg is legjobban szabályozott szektor, a pénzügyi szektor intézményeiben régóta alkalmazzák. Ezen eljárások felölelik az intézmények IT kockázatelemzését is. A leggondosabb eljárások mellet is marad azonban bizonyos szintű maradvány kockázat, mivel tökéletes biztonság nincsen, vagy éppen a közel 100%os biztonsági szint megteremtése irreális költségekkel lenne csak megvalósítható.

Jelen jegyzet célja ennek megfelelően áttekintő képet adni a kockázatmenedzsment IT-hoz kapcsolódó speciális részterületéről, kapcsolódásairól más területekkel.

A témában szűkösen rendelkezésre álló magyar nyelvű szakirodalomi források sokszor jelentős átfedést mutattak egymással, így ahol nem szó szerinti idézés történt, ott a felhasznált irodalmak listája az irodalomjegyzékben megtalálható. A jegyzet feltünteti az angol fogalmakat is a terminológia pontos használatának érdekében, mivel az irodalom nyelve elsődlegesen az angol.

1 Fogalmi keretrendszer

„The beginning of wisdom is the definition of terms.”

(Socrates)

Az informatikai kockázatelemzés területén fontos az alapfogalmak pontos ismerete és használata. Ezeket a fogalmakat más területeken, esetleg más-más értelemben, vagy kissé módosított jelentéssel használják, ennek érdekében ez a fejezet a fogalmi keretrendszert mutatja be, elsősorban az Ibtv-t és a hozzá kapcsolódó jogszabályokból átvett fogalommagyarázatot alkalmazva, azt kiegészítve. Az ebben a fejezetben nem definiált fogalmak az első előfordulásuk alkalmával kerülnek meghatározásra.

A *kockázat (risk)* definíciójára a különböző területeken számos meghatározás létezik. A kockázat információhiányt jelöl. IT kockázat megközelítésmódjából kockázat (R) a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének, W) és az ez által okozott kár nagyságának/súlyosságának (K) a függvénye. Matematikai megközelítésben: $R = W \times K$.

A *fenyegetés, fenyegetettség (threat)* olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemeinek védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát.

A *kockázatelemzés (risk analysis)* az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

A *kockázatkezelés (risk treatment)* a kockázatok csökkentésére vonatkozó intézkedések kiválasztására és végrehajtására vonatkozó folyamat. Kockázatkezelési intézkedések közé tartozik a kockázat elkerülése, optimalizálása, átadása vagy a kockázat tudatos felvállalása, elviselése. Az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása.

A *kockázatokkal arányos védelem (Balancing Risk and Controls)* az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

A kockázatértékelés, és a *kockázatfelmérés (risk assessment)* esetén mindkét magyar kifejezés angol eredetije az ’assessment’.

Kockázatmenedzsment (risk management) a vezetési elvek, tapasztalatok és eljárások rendszeres alkalmazása a kockázatok azonosítására, megfigyelésére, elemzésére, felmérésére és csökkentésére.

Sérülékenység (vulnerability) az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.

Sérülékenység-vizsgálat *(Vulnerability and penetration testing; vulnerability assessment)* az elektronikus információs rendszerek gyenge pontjainak (biztonsági réseinek) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.

Üzletmenet folytonossági terv (Business Continuous Plan, BCP) a kritikus üzleti folyamatokban beálló zavar esetén a szervezet által használt reagálási terv.

Katasztrófa-elhárítási terv (Business Recovery Plan, DRP) a tevékenységek katasztrófa, vagy vészhelyzet által történő megszakadása esetén alkalmazandó emberi, fizikai, technikai és adminisztratív eljárások összességét tartalmazó terv, amely a szolgáltatások meghatározott idő- és költségkereten belül történő helyreállítását szolgálja.

PreDeCo elv a védelmet (kontrollok) három egymásra épülő és egymást kiegészítő részekre bontó módszertan.

Információbiztonság[2,3] *(information security)* szélesebb körben értelmezett, mint az informatikai biztonság. Az adatok védelmére fókuszál – attól függetlenül, hogy azok elektronikus, informatikai rendszerben, vagy más módon kezelt adatok

Informatikai biztonság (Information Security, InfoSec) az információbiztonság részhalmaza, számítógépes biztonság. Az informatikai rendszerekben kezelt adatok védelmén túl az adatokat kezelő, tároló, továbbító rendszer védelmét is jelenti.

1.1 Az információbiztonság alappillérei

Az információbiztonság az a folyamat, melynek során az információkat megvédjük a nem engedélyezett hozzáféréstől, használattól, felfedéstől, kiszivárgástól, megsemmisítéstől, módosítástól, és megzavarástól.

- ✓ MIT kell védenünk? – Vagyonleltár.
- ✓ MITŐL? – Kockázatok azonosítása.
- ✓ HOGYAN? – Fizikai, logika, adminisztratív szabályzók, szabályzatok.

[2] Bővebben lásd: Cherdantseva (2014)

[3] Az Ibtv. megfogalmazása mind az információbiztonság, mind az informatikai biztonság megközelítésmódját alkalmazza.

Az információbiztonság alappilléreinek tekintett *bizalmasság (Confidentiality), sértetlenség (Integrity), rendelkezésre állás (Availability)* angol kifejezéseinek kezdőbetűinek összeolvasásából a módszertant CIA módszertanként szokták nevezni. A legfrissebb megközelítések ezt a modellt kiegészítik a *felelősségre vonhatóság, elszámoltathatóság (Accountability)* tényezőjével, ami a tevékenységek nyomon követhetőségének szükségességét jelenti a felelős forrásig. (Wheeler, 2011, p. 10)

Bizalmasság (Confidentiality) 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.

Sértetlenség (Integrity) 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.

Rendelkezésre állás (Availability) annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

Az Ibtv. hatálya alá tartozó elektronikus információs rendszerek *teljes életciklus*ában meg kell valósítani és biztosítani kell: az elektronikus információs rendszerben kezelt *adatok* és *információ*k *bizalmassága*, *sértetlensége* és *rendelkezésre állása*, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása *zárt*, *teljes körű*, *folytonos* és *kockázatokkal arányos védelmét*.[4]

Teljes életciklus (life cycle) az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam.

Zárt védelem az összes számításba vehető fenyegetést figyelembe vevő védelem.

Folytonos védelem az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.

Teljes körű védelem az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.

[4] Ibtv. 5§

1.2 Védelemi intézkedések, szintek

Az elektronikus információs rendszernek az Ibtv. 5. §-ban meghatározott feltételeknek megfelelő védelme érdekében a szervezetnek külön jogszabályban[5] előírt *logikai, fizikai* és *adminisztratív védelmi* intézkedéseket kell meghatároznia, amelyek támogatják a *megelőzés*t és a *korai figyelmeztetést,* az *észlelés*t, a *reagálás*t, és a *biztonsági események kezelésé*t.

A védelmi intézkedéseket rendszerszemlélettel kell vizsgálni tekintettel arra, hogy az egyes védelmi intézkedések egymás hatását erősíthetik, illetve gyengíthetik, továbbá egy rendszer annyira erős, mint a leggyengébb eleme. A hatékony, egyenszilárdságú védelem megteremtése a cél, amelynek előfeltétele a legalább azonos erősségű védelmi intézkedések alkalmazása.

Logikai védelem (Logical controls) az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.

A logikai védelem kategóriájába tartozik többek között a hozzáférés szabályozásának technológiai szintű megvalósítása, a tűzfalak, authentikációs rendszerek, PKI infrastruktúra használata, VPN, tartalomszűrés, vírusvédelem, mentési/archiválási rendszerek használata.

Fizikai védelem (Physical controls) a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.

Adminisztratív védelem (Administrative/Procedural controls) a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.

Az adminisztratív védelem magába foglalja a különböző eljárásrendi védelmeket, az informatikai stratégia, az informatikai biztonsági politika, szabályzat, üzletmenet folytonossági és katasztrófa elhárítási terveket is.

[5] 77/2013. (XII. 19.) NFM rendelet

2 A kockázatértékelés, a kockázatelemzés, és a kockázat-menedzsment kapcsolata

A *kockázatértékelés*nek (*kockázatfelmérés*nek), az elemzésnek és menedzselésnek igazodnia kell a vizsgált intézmény üzleti folyamataihoz, ki kell terjednie az IT rendszerek *teljes életciklus*ára és fel kell ölelnie a kiszervezés és az ellenőrzés területét is.

A *kockázatelemzés* – a kockázatértékelés részeként – az IT biztonság lényeges eleme, azonban annak rendszeres kivitelezését megnehezíti a rendszerek a környezet és az emberek bonyolult interdependenciája.

Annak érdekében, hogy ez a kölcsönös függőség kezelhető legyen, módszertanra van szükség. A választott módszertannal szemben az Ibtv-hez kapcsolódó 77/2013. (XII. 19.) NFM rendelet megfogalmazása szerint: „a kockázatelemzés során ajánlott a nemzetközi vagy hazai szabványok, ajánlások, legjobb gyakorlatok figyelembevétele."

A módszertannal szemben annyi elvárást érdemes támasztani, hogy az megfelelően megbízható, azaz a kockázatok szisztematikus felmérésére alkalmas legyen.[6]

Összefoglalva a *kockázatmenedzsment* folyamata több lépésből áll, melynek fontosabb részterületei, elemei általában a következőek:

- Kockázatértékelés
  - A kockázat azonosítása – a potenciális kedvezőtlen (üzleti) hatások felmérése.
- Kockázatelemzés (a kockázatértékelés része)
  - A vagyontárgyak azonosítása és értékelése;
  - a fenyegetések felmérése;
  - a sebezhetőségek felmérése;
  - a kockázatok felmérése, értékelése;
  - elfogadható kockázati szint meghatározása, a kockázatokhoz kapcsolódó lehetséges reakciók azonosítása;
  - a kockázatokra adható válaszok mérlegelése.
- Kockázatkezelés
  - A meglévő/tervezett válaszintézkedések/ellenintézkedések meghatározása;
  - a válaszintézkedés beépítése, és a kialakított keretrendszer rendszeres felülvizsgálata.

[6] Az 1. mellékletben megtalálható az Európai Unió Hálózati és Információ Biztonságért felelős Hivatala (ENISA) által összeállított módszertanok listája.

3 Kockázatértékelés

Az informatikai rendszerek biztonságának megteremtése elsősorban szervezési és csak azt követően technikai kérdés. Ennek megfelelően a kockázatok feltárásának területén is rendszerszemléletű megközelítést kell alkalmazni; fel kell mérni a szervezet folyamatait – ügyfolyamatait is beleértve, – környezetét, partnerkapcsolatait, a folyamatokat kiszolgáló, illetve biztosító informatikai rendszereket, amelyekre vonatkozóan további külön szempontrendszer alapján végezzük a kockázatok feltárását, elemzését. A helyzet feltárása, elemzése alapján lehet csak – a jogszabályi környezethez illeszkedően – szakmailag és gazdaságilag is megalapozott a védelem kialakítása.

Amint a fenti megfogalmazásból is látható, a kockázatelemzés területén több terület együttműködése szükséges, több szakág képviselőinek kell képviseltetniük magukat, az elemzés elvégzése nem lehet csak az IT feladata. A későbbiekben ismertetésre kerülő üzletmenet-folytonossági terv elkészítése is szélesebb spektrumban értelmezendő – mintsem csak az IT felelősségi területe. Az üzletmenet-folytonossági terv az üzleti folyamat bármilyen okból történő kiesése, sérülése esetére dolgoz ki alternatív eljárást a probléma elhárításának idejére – beleértve akár a kieső informatikai szolgáltatás átmeneti kiváltását is. Ezen megközelítésmód alapján a terv elkészítése – az IT felelősségi területeit meghaladóan szélesebb körben értelmezendő, azonban ahhoz szükséges az IT támogatása és szempontrendszerei is. Ennek ellenére ezt sokszor teljes mértékben az IT hatáskörébe utalják. A kockázatértékelés és az üzletmenet-folytonosság biztosításának egyik alapfeltétele a jól meghatározott folyamatok és a folyamatok kapcsolatainak ismerete.

A kockázatazonosítás célja annak megállapítása, hogy melyek a szervezet célkitűzéseit, és működését veszélyeztető fő kockázatok. A szervezetre vonatkozó „általános”, és a szervezeten belüli IT kockázatokat egymással szoros összefüggésben kell kezelni.

A kockázatok csoportosítása több szempont alapján történhet. A kölcsönös inter- és intradependenciák (hierarchikus függőségek) miatt az informatikai kockázatok ábrázolása szinte lehetetlen más kockázat kategóriák függvényében. Mindemellett az áttekintéshez jó kiindulópont lehet az 1. ábrán látható – pénzügyi szektor orientált – megközelítés a kockázatok hierarchiájára és a kapcsolódó IT kockázatokra.

Forrás: *ISACA, 2009, p. 11 alapján*

1. ábra ***IT kockázatok elhelyezkedése a kockázatok hierarchiájában***

Stratégiai kockázatok lehetnek a stratégia nem megfelelő végrehajtása, alkalmazása, vagy a nem megfelelően megválasztott stratégia, vagy a stratégia hiánya.

Környezeti kockázatok a szervezet működésére hatást gyakorló belső kockázatok, – amelyekre – bizonyos mértékben – hatást tud gyakorolni a szervezet, illetve a szervezet ellenőrzésén, befolyásán kívül eső külső kockázatok, például elemi csapások.

Piaci (és ügyfelekkel kapcsolatos) kockázatok lehetnek a szállítói probléma, az ügyféligények változása, vagy az ügyféligények nem megfelelő kezelése.

Pénzügyi kockázatok lehetnek költségvetési – a szükséges fedezet hiánya, a megkívánt tevékenység ellátására nem elég a rendelkezésre álló forrás; biztosítási – a biztosítás elmulasztása, mivel a megfelelő biztosítás nem érhető el elfogadható költségen; beruházási – nem megfelelő beruházási döntések meghozatala; illetve felelősségvállalási – mások cselekedete által, a szervezetre gyakorolt negatív hatás következtében felmerülő kártérítések.

Működési kockázatok lehetnek az emberek, a belső folyamatok és rendszerek nem megfelelő vagy hibás működése, illetve külső tényezők által előidézett veszteségek kockázata. A működési kockázatok kiemelt területe az informatika.

Megfelelőségi kockázat (compliance) a szervezet külső és belső tevékenységét tekintve a vonatkozó bonyolult és folyamatosan változó jogszabályok, illetve jogszabálynak nem minősülő egyéb előírások – ajánlások, irányelvek, módszertani útmutatók – be nem tartása következtében esetlegesen keletkező jogi vagy hatósági bírság, szankció, pénzügyi veszteség, vagy hírnévromlás kockázata.

Az IT értékteremtését fenyegető kockázatok azok, amelyek – az üzleti folyamatok hatékonyságának növelése érdekében – a technológia értékteremtést biztosító használatát veszélyeztetik.

Az IT munkaterv és megvalósítási kockázata az új, vagy továbbfejlesztett üzleti megoldásokhoz történő IT hozzájárulás megvalósulását fenyegeti.

IT működés és szolgáltatásnyújtási kockázat az IT rendszerek és szolgáltatások teljesítményével kapcsolatos valamennyi kockázat.

Az ebben a lépésben azonosított kockázatoknak az üzletmenet-folytonossági terv és az ahhoz szorosan kapcsolódó katasztrófa-elhárítási terv készítése folyamán lesz fontos szerepe.

4 Kockázatelemzés[7]

A kockázatelemzés segítséget nyújt abban, hogy a rendszer leggyengébb pontjait, a legnagyobb kockázatot jelentő fenyegetettségeket (veszélyforrásokat) azonosítani lehessen és ennek ismeretében költséghatékony, *kockázatarányos védekezés*t lehessen kialakítani. Megfelelően megalapozott kockázatelemzés hiányában nem biztosított, hogy a biztonság fokozására fordított kiadások a leghatékonyabban kerülnek felhasználásra.

A kockázatelemzés az IT biztonság megteremtésének nélkülözhetetlen, lényeges eleme. A bonyolult IT és üzleti/ügyfolyamatok összefonódása miatt a kockázatok és a konkrét kárértékek számszerűsíthetősége problematikus, így általában olyan összehasonlításra lehetőséget adó eljárások, elemzések kerülnek alkalmazásra, amelyek alapján a legcélszerűbb védelmi intézkedések meghatározhatóak.

Általánosságban elmondható, hogy nincs jó, vagy rossz módszertan. A kockázatmenedzsment területén alkalmazandó módszertan kiválasztása során arra kell ügyelni, hogy a választott módszer a szervezet számára kényelmes, megbízható és folyamatosan elvégezhető legyen, a korábbi és a jövőbeli állapotokkal összevethető eredményt hozzon.

A módszertanok lehetnek kvalitatív, kvantitatív, semi-kvantitatív megközelítésűek. A legtöbb módszer táblázatokat használ a kockázatok felsorolására és priorizálására, kombinálva azokat szubjektív és tapasztalati mutatószámokkal. Az ebben a fejezetben

[7] A 77/2013. (XII. 19.) NFM rendelet 1. mellékletének, az elektronikus információs rendszerek biztonsági osztályba sorolására vonatkozó releváns szövegkörnyezetét kiindulási pontként vesszük alapul a fejezetben.

bemutatott eljárás egy egyszerűsített táblázatos módszert mutat be, amely azonban az összetettebb módszertanokhoz is jó kiindulópontot biztosít.[8]

A kockázatmenedzsment néhány nehezítő tényezője közé tartozik, hogy

- ✓ Nem ismerjük az összes veszélyt, kockázatot;
- ✓ nem ismerjük az adott veszély bekövetkezési valószínűségét;
- ✓ nem ismerjük a veszély bekövetkeztekor fellépő kár nagyságát.

Éppen ezért szükséges

- ✓ A veszélyforrások listájának összeállítása (kimaradt kockázatok „maradék kockázat”),
- ✓ valószínűségi kategóriák alkalmazása;
- ✓ átlagos (becsült) kárérték kategóriák megfogalmazása.

Csak a „lényeges” kockázatokkal foglalkozunk.

„Bármilyen kockázatelemzési tevékenység megkezdése előtt a szervezetnek stratégiával kell rendelkeznie az ilyen elemzésekhez és ennek összetevőit (eljárások, technikák s a többi) dokumentálni kell az informatikai biztonságpolitikában.” (KIB 25. számú ajánlása, IBIK, p. 27)

Az elérhető módszertanok közös jellemzője, hogy a következő kockázatelemzési lépéseket tartalmazzák:

1. A kockázatok azonosítása, veszélyforrások listájának összeállítása.
2. A bekövetkezési valószínűség megállapítása.
3. Lehetséges károk és értékük meghatározása.
   (A CIA kategóriáknak megfelelően.)
4. Kockázati tényezők származtatása.
   (Kárérték meghatározása „kockázati szorzótábla” alapján.)
5. Kockázatok kezelése/Védelemi intézkedések számbavétele.

4.1 A kockázatok azonosítása, veszélyforrások listájának összeállítása

A kockázatmenedzsment program kezdeti lépéseként azon fenyegetések, sebezhetőségek, események, cselekmények és kockázatok forrásainak – továbbiakban összefoglalóan veszélyforrások[9] – átfogó listáját kell létrehozni, amelyek a szervezet céljainak

[8] A bemutatott eljárás a Biztostű.hu (2004) forrásra nagyban támaszkodik, azt kiegészíti.

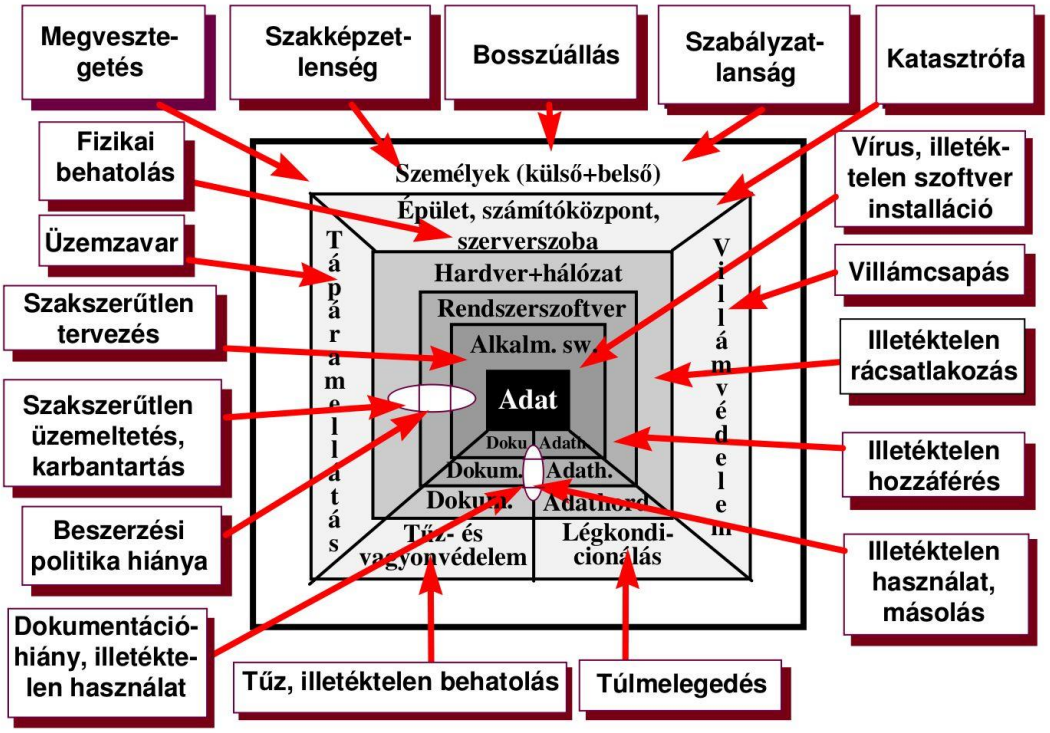
[9] Az informatikai szaknyelvben sokszor okoz nehézséget, pontatlanságot a többes jelentéssel bíró angol szakkifejezések magyar nyelvű megfelelőinek használata. Igaz ez arra az esetre is, ha magyarul használunk többes, árnyaltabb jelentéstartalmú kifejezéseket ugyanarra a jelenségkörre. A kockázatelemzés területén

elérésére hatással lehetnek. Az információs erőforrásokkal szembeni veszélyeket, fenyegetettségeket és azok bekövetkezési valószínűségét kell értékelni. A veszélyforrások jelentősen eltérőek lehetnek a kisebb súlyú csalásoktól a katasztrofális hatású természeti csapásokig.

Ebben az összefüggésben a fenyegetések olyan körülményeket vagy eseményeket jelentenek, ami kárt okozhat az elektronikus információs rendszerben előforduló/meglévő sérülékenység kihasználásával.

Az adatok és az adott információs rendszer jellegéből kiindulva a kockázatelemezés alapját:

- ✓ Az adatok *bizalmasság*ának, *sértetlenség*ének és *rendelkezésre állás*ának, és az elektronikus információs rendszerelemek *sértetlenség*ének és *rendelkezésre állás*ának sérüléséből, elvesztéséből bekövetkező kár, vagy káros hatás, terjedelme, nagysága;
- ✓ a kár bekövetkezésének, vagy a kárral, káros hatással fenyegető veszély mértéke, becsült valószínűsége képezi.[10]



Forrás: *ITB 12. ajánlás p.16*

2. ábra *Védelmi intézkedések, fenyegetettségek*

veszélyforrásnak nevezzük a rendszer elvárt (helyes) és biztonságos működését fenyegető eseményeket. (Vegyük észre, hogy ez a kifejezés az Ibtv. törvényben megtalálható fenyegetés definíciójának átfedése, összefoglalása, kiterjesztése, amely tartalmazza a „művelet", az „esemény", és a „cselekmény" fogalmait.)

[10] 77/2013. (XII. 19.) NFM rendelet 1. melléklet 1.2.1. pontja

Első lépésként erőforrás leltár készítése szükséges, amelyhez nélkülözhetetlen a vagyontárgyak azonosítása.

4.1.1 Vagyontárgyak azonosítása, erőforrás lista

Az üzleti és az IT folyamatok alapja az információ, amelynek alapja az adat. Az adatok sérülése, megsemmisülése, felfedése veszélyeztetheti a működést és súlyos károkat okozhat. A vagyontárgyak azonosítása, az adatvagyon felmérése biztosítja, hogy megismerjük az adatok előfordulási helyét, felhasználásának sajátosságait, a szervezet folyamataihoz való kapcsolódását. Az adatvagyon felmérés biztosítja a védelemszervezés alapját is.

A vagyontárgyak azonosítására a hatályos magyar joganyagból egy rendelet[11] adhat kiindulópontot, amelynek alapján az adatvagyon-leltár a következő részekből áll:

a*) információ-vagyon*: adatok (az adatok biztonsági osztályozása szerint), adatbázisok, szoftver-kezelési kézikönyvek, oktatási, üzemviteli, üzemeltetési, biztonsági segédletek és nyilvántartások;

b) *szoftver-vagyon*: rendszer-szoftverek, alkalmazói szoftverek, fejlesztő-eszközök;

c) *fizikai-vagyon*: hardver (számítógépek, perifériák, mobil számítástechnikai eszközök), kommunikációs eszközök (telefonok, faxok, modemek, hálózati csatoló eszközök, telefon-alközpontok), adathordozók és egyéb műszaki berendezések (szünetmentes tápegység, légkondicionáló berendezés, villámhárító stb.).

A jogszabály alapján azonosíthatjuk az adatvagyont, azonban erőforrás alatt nem csak az adatvagyont, hanem minden, az informatikai működést megvalósító, arra valamilyen befolyással bíró erőforrást számításba kell venni. A teljes kockázatelemzés elvégzése érdekében a humán erőforrással is számolnunk kell, ami egyrészt erőforrás, másrészt egyben kockázati tényező is, mind belső, mind külső oldalról. Példaként a social engineering említhető, amely kockázat az emberi oldalon leselkedik a rendszer integritása terén.

A leltár elkészítésekor kell felmérni és dokumentálni az egyes erőforrások kapcsolatait, a rendszer topológiáját is.

4.1.2 A sérülékenységek – sebezhetőségek

Amint azt a bevezetőben is említett Secunia jelentés is kiemelte, a fő veszélyforrás a sérülékenységek nem megfelelő kezelése. A sérülékenység fogalmára sokszor, mint bináris állapotra vonatkozó fogalomként tekintenek. Valami „sérülékeny”, vagy „nem sebezhető”.

[11] 21/2010. (V. 6.) IRM-MeHVM együttes rendelet – a fizetési meghagyásos eljárás lefolytatásának támogatására szolgáló informatikai rendszer informatikai biztonsági követelményeiről (12. rész 24.§-a alapján)

Még pontosabban, az eszközök különböző mértékben vannak kitéve a sérülékenységnek – az adott üzemeltetési körülmények függvényében jelenthetnek nagyfokú kiszolgáltatottságot, vagy alacsonyabb fokú biztonsági rést.[12] Ez a megkülönböztetés a továbbiakban fontos alapot jelent a kockázati szint meghatározásának területén, valamint a következtetések és javasolt beavatkozások megfogalmazásakor.

Néhány példa a sérülékenységre: hibás szoftver, nem megfelelően konfigurált berendezés, gyenge hálózat kialakítása, titkosítás nélküli adatátvitel, nem megfelelő karbantartás, nem tesztelt technológia alkalmazása, redundancia hiánya, biztonsági hiányosságok, rossz jelszavak, nem megfelelő személyzet, a felhasználói támogatás hiányosságai, ellenőrizetlen, vagy hibás folyamatok, a szabályozások nem megfelelő kezelése, „kikényszerítése", vezetés kommunikációs hibái.

4.1.3 Veszélyforrások csoportosítása

Korábban a kockázatok csoportosításánál is megfigyelhettük, hogy a veszélyek csoportosítása, az azokban szereplő kategóriák meghatározása sem egyértelmű. A veszélyek csoportosítására több lehetőség is kínálkozik a szakirodalom alapján. Egyik lehetséges megközelítés a természeti (árvíz, tűz, s a többi), véletlen (tűz, víz, épületkár, s a többi), szándékos fizikai (tűz, víz, terrortámadás, s a többi), szándékos nem fizikai (csalás, adathalászat, social engineering, s a többi) csoportosítás. (ISACA, 2012, p. 10)

A következő kategorizálás jobban alkalmazható az eddig tárgyaltak figyelembe vételével, mivel ennek alkalmazásával a válaszintézkedések területei besorolhatóak a *fizikai, logikai vagy az adminisztratív védelem* kategóriáiba, valamint kiemeli a belső humán erőforrás szerepét is.

- ✓ *Természeti* veszélyforrások (például tűz, csőtörés, árvíz, villám, földrengés).
- ✓ *Adminisztratív* (szervezési) gyengeségek (szervezési hiányosságokból eredő veszélyek).
- ✓ *Fizikai* veszélyek (például betörés, lopás, rongálás, (hardver, adathordozó, adatátvitel) meghibásodásai).
- ✓ *Logikai* fenyegetések (például informatikai csalás, hálózati betörés, lehallgatás, jogosulatlan módosítás, vírusfertőzésből adódó működésképtelenség, adatvesztés, szoftver hibából, rendszer helytelen kezeléséből adódó működésképtelenség).
- ✓ *Humán* veszélyforrások (például belső munkatársak gondatlansága, visszaélések).

[12] Kontextusban erre vonatkozóan lásd 77/2013. (XII. 19.) NFM rendelet biztonsági osztályba sorolás részét.

A szervezet belső és külső környezetének, folyamatainak ismerete nagyon fontos a veszélyforrások és a kockázatok azonosításában. Az IT kockázatkezeléshez az egész szervezet folyamatait és kockázatait kell alapul venni.

4.1.4 Veszélyforrások feltárásának módszerei

A veszélyforrások feltárása az eddigi tapasztalatok felhasználásával, illetve a rendszer elemzéséből felderített hiányosságok számbavételével történhet. Az egyes veszélyforrásokat, kockázatokat helyzetfelméréssel tudjuk meghatározni. A helyzetfelmérés történhet:

- ✓ Dokumentumok elemzésével (a rendszer tervezési felülvizsgálata, rendszertervek elemzése, szabályzatok, dokumentációk vizsgálata);
- ✓ interjúkkal, csoportos módszerekkel;
- ✓ „mi lenne, ha” és forgatókönyv-elemzés módszerével (a stratégiai kockázatok és a folyamatok azonosítására);
- ✓ szemlével.

A veszélyforrások listájának összeállításakor törekedni kell a legtöbb számításba jöhető veszélyforrás azonosítására. Az esetleg kimaradó veszélyforrásokat maradék kockázatként kezelhetjük.

A bemutatásra kerülő táblázatos módszer esetében a veszélyforrások listája alkotja a kockázatelemzési tábla egyes sorait. A későbbi könnyebb azonosíthatóság érdekében egy, a kockázatcsoportra utaló azonosítóval érdemes ellátni az egyes veszélyforrásokat. (Például H1 első humán veszélyforrás, H2 második számú feltárt humán veszélyforrás.) A kockázatelemzési táblázat többi részének jelentése, kitöltése a következő lépésekben kerül bemutatásra.

1**. táblázat** ***Kockázatelemzési táblázat***

ID	**Veszélyforrás**	**Bekövetkezés valószínűsége**	**Kár**			**Kockázat**	**Védelmi intézkedés**
		P	C	I	A	R	V
H1	social engineering						
…							

Forrás: *Biztostű.hu, 2004 alapján*

4.2 A bekövetkezési valószínűség megállapítása

Nagyon fontos a bekövetkezési valószínűség nagyságrendi megállapítása. Figyelembe kell venni az események *bekövetkezési valószínűség*ét, illetve szándékos visszaélések esetén az úgynevezett *támadási potenciál*t.

A *bekövetkezési valószínűség* becslése az addigi tapasztalatok – ha rendelkezésre áll, statisztikai adatok – alapján történik (például villámcsapásra néhány évente, míg vírusfertőzésre akár havonta is számíthatunk).

A *támadási potenciál* meghatározásánál figyelembe kell venni a gyengeség kihasználásához szükséges támadói felkészültségi szintet, valamint, hogy mennyire érdemes támadást végrehajtani az adott rendszer ellen. A szükséges felkészülési szintek alapján lehet

- ✓ Automatizált eszközzel végrehajtható,
- ✓ átlagos felhasználó által kihasználható,
- ✓ átlagos felhasználó által, instrukciók alapján kihasználható,
- ✓ csak programozói tudással kihasználható,
- ✓ profi támadót igénylő gyengeség.

2. táblázat *Bekövetkezési valószínűségek*

Jelölés	Angol név	Magyar név	Gyakoriság, illetve támadási potenciál
PVS	very small	nagyon kicsi	ritkán, kb. 10 évente egyszer várható az előfordulása
PS	small	kicsi	kb. 5-10 évente előforduló, vagy csak profi támadó által kihasználható gyengeség
PA	average	közepes	éves távlatban előforduló, vagy átlagos szakember által kihasználható gyengeség
PL	large	nagy	évente egyszer előforduló, vagy átlagos szakember által végrehajtható visszaélés
PVL	very large	nagyon nagy	évente többször előforduló, vagy bárki által kihasználható gyengeség

Forrás: *Biztostű.hu, 2004 alapján*

A veszélyforrások bekövetkezési valószínűségének, illetve a gyengeség kihasználásához szükséges támadási potenciálnak a becslése a kockázatelemzési táblázat „P” (probability) oszlopának megfelelő kitöltésével történik.

3. táblázat *Kockázatelemzési táblázat – bekövetkezési valószínűségek*

ID	Veszélyforrás	Bekövetkezés valószínűsége	Kár			Kockázat	Védelmi intézkedés
		P	C	I	A	R	V
H1	social engineering	PVL					
…							

Forrás: *Biztostű.hu, 2004 alapján*

4.3 Lehetséges károk és értékük meghatározása

Információbiztonsági incidens esetén a lehetséges károkat közvetlen és közvetett kategóriákba csoportosíthatjuk. A károk lehetnek elsődleges, másodlagos, illetve harmadlagos károk. Az elsődleges kár az adott rendszerben felmerült tényleges kár mértéke, a helyreállítás költsége. A másodlagos és harmadlagos kár a láncreakción, kölcsönhatásokon keresztül, a teljes szervezetben realizálódott veszteség mértéke. (Póserné, 2007) Közvetlen kár lehet az adatvesztés, rendszerleállás, hardver és szoftverkárok, adatok illetéktelen kezekbe jutása. A közvetett, vagy akár elvi kár is keletkezhet, amely nem számszerűsíthető, például bizalomvesztés az adott szervezettel szemben.

Egy adathordozó sérülése esetén az elsődleges kár, az adathordozó pótlása/cseréje jelentősen kevesebb értéket képviselhet, mint az azon tárolt adatok pótlása/megsemmisülése (biztonsági mentés meglétének kérdésköre), vagy nyilvánosságra kerülése (például adatmentést végző cégtől történő adatszivárgás) által okozott kár.

A 77/2013. (XII. 19.) NFM rendelet 1. mellékletének 1.4 pontja alapján az elektronikus információs rendszerek biztonsági osztályainak meghatározásához az alábbi – az érintett szervezetnél szóba jöhető – közvetett, vagy közvetlen kárt okozó hatásokat, veszélyeket és károkat kell – az érintett szervezet jellemzőire tekintettel – figyelembe venni:

- ✓ *társadalmi-politikai káros hatásokat, károkat vagy a jogsértésből, kötelezettség elmulasztásából fakadó káros hatásokat, károkat* (így például alaptevékenységek akadályozása, különösen a létfontosságú információs rendszerelemek működési zavarai, a nemzeti adatvagyon sérülései, jogszabályok és egyéb szabályozások megsértése, jogszabály által védett adatokkal történő visszaélés vagy azok sérülése, a közérdekűség követelményének sérülése, személyiséghez fűződő jogok megsértése, bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben, az ország jogrendjének sérülése, vagy ennek lehetővé tétele);
- ✓ *személyeket, csoportokat érintő károk, káros hatások* (például különleges személyes adatok, banktitkok, üzleti titkok megsértése, szervezet, személyek vagy csoportok jó hírének károsodása, személyi sérülések, vagy haláleset bekövetkeztének – ideértve az elektronikus információs rendszer működésének zavara, vagy információhiány miatt kialakult veszélyhelyzetet – veszélye);
- ✓ *közvetlen anyagi károk* (az infrastruktúrát, az elektronikus információs rendszert ért károk, és ezek rendelkezésre állásának elvesztése miatti pénzügyi veszteség, adatok sértetlenségének, rendelkezésre állásának elvesztése miatti költségek, dologi kár);

- ✓ *közvetett anyagi károk* (például helyreállítási költségek, elmaradt haszonnal arányos költségek, a környezet biztonságának veszélyeztetése, perköltségek).

A különböző veszélyforrások bekövetkezése esetén keletkező károk meghatározása komplex feladat. Egy nagyobb, összetett informatikai rendszerben az egyes rendszerelemek bonyolult függőségi viszonyban állnak egymással, így egy adott rendszerelem sérülése esetén végig kell követni a többi rendszerelemre és üzleti folyamatokra kifejtett hatását.

4. táblázat *Kárkategóriák meghatározása*

Jelölés	Angol név	Magyar név	Magyarázat
DVS	very small	elhanyagolható	elsődleges, kis összegű kár
DS	small	kicsi	másodlagos, nagyobb összegű kár
DA	average	közepes	fennakadás az alkalmazói rendszerben, könnyű emberi sérülés
DL	large	nagy	komoly fennakadás az üzleti/ügy-folyamatokban, súlyos emberi sérülés
DVL	very large	nagyon nagy	az üzletmenetben időleges fennakadás, ügyfélkörben is érezhető változás, haláleset
DD	disaster	katasztrofális	az üzletmenet hosszabb megszakadása, bizalomvesztés, komoly társadalmi hatású probléma,

Forrás: *Biztostű.hu, 2004*

A 3. mellékletben megtalálható a KIB 25. számú ajánlása: 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR)-ben szereplő lehetséges kárérték táblázat.

5. táblázat *Kárérték táblázat*

Jelölés	Angol név	Magyar név	Magyarázat
RVS	very small	nagyon kicsi	10 ezer Ft/év
RS	small	kicsi	100 ezer Ft/év
RA	average	közepes	1 millió Ft/év
RL	large	nagy	10 millió Ft/év
RVL	very large	nagyon nagy	beláthatatlan (nem korlátos)

Forrás: *Biztostű.hu, 2004*

Tekintve, hogy az informatikai rendszereket, a bennük tárolt információkat jelentősen eltérő hatásmechanizmusú veszélyek fenyegetik (például más a hatása egy titkos információ kiszivárgásának, mint egy adathordozó megsérüléséből származó adatvesztésnek) figyelembe kell venni az okozott kár természetét is, illetve azt, hogy az érintett rendszerelem milyen tulajdonsága sérült a CIA elv alapján.

Ennek megfelelően a károk meghatározását a következő szempontok szerint vizsgáljuk:

- ✓ Bizalmasság megsértése, jogtalan információszerzés,

- ✓ sértetlenség elvesztése, a tárolt adatok manipulálása,
- ✓ rendelkezésre állás elvesztése.

Ezután a meghatározott kárkategóriáknak megfelelően töltjük ki a kár CIA oszlopait, ahol az szükséges. Például az áramszünet nem okozza a bizalmasság sérülését, de hatással van a rendelkezésre állásra, valamint következtében akár a tárolt adatok is sérülhetnek; ezt a hatásmechanizmust az I és A oszlopok megfelelő kitöltésével, a C oszlopban kihúzással jelölhetjük.

6. táblázat *Kockázatelemzési táblázat – kár CIA kategóriáknak megfelelően*

ID	Veszélyforrás	Bekövetkezés valószínűsége	Kár			Kockázat	Védelmi intézkedés
		P	C	I	A	R	V
H1	social engineering	PVL	DD	DVL	DD		
…				3. (aktuális) lépés			
F1	áramszünet	PVL	-	DS	DA		

Forrás: *Biztostű.hu, 2004 alapján*

4.4 Kockázati tényezők származtatása

A kockázati tényezők származtatásakor „nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni”,[13] amint azt a 77/2013. (XII. 19.) NFM rendelet is megfogalmazza a rendszerek biztonsági osztályba sorolásakor.

A bemutatott eljárás során ezt a kockázati szorzótáblával tudjuk elérni. A szorzótábla sorát a veszélyforrás előfordulási gyakorisága, oszlopát általában a CIA szempontok közül a legnagyobb kárral járó kár kategóriája határozza meg. Az így meghatározott sor és oszlopnak megfelelő cella tartalmazza a kockázatot. Így a kockázatelemzési tábla „R” oszlopának kitöltése gyakorlatilag automatikus. Egyes módszertanok megengedik, hogy speciális esetekben a kockázatelemzést végző szakértő megfelelő indokok alapján az így meghatározott kockázati kategórián korrigáljon, ezzel kezelve le az elnagyolt, kategória alapú becslési folyamat esetleges hibáit.[14]

[13] 77/2013. (XII. 19.) NFM rendelet 1. melléklet 1.3. pontja

[14] Az Ibtv. is lehetőséget biztosít például biztonsági osztályba sorolás esetén a szervezet vezetője részére, aki a „törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes esetben indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.”

7. táblázat *Kockázati szorzótábla*

Kár / P	DVS	DS	DA	DL	DVL	DD
PVS	RVS	RVS	RS	RA	RL	RVL
PS	RVS	RS	RA	RL	RVL	RVL
PA	RVS	RS	RA	RL	RVL	RVL
PL	RV	RS	RA	RL	RVL	RVL
PVL	RS	RS	RL	RVL	RVL	RVL

Forrás: *Biztostű.hu, 2004 alapján*

A kockázat oszlopot a fent meghatározott kockázati szorzótábla segítségével töltjük ki.

8. táblázat *Kockázatelemzési táblázat – Kockázat*

ID	Veszélyforrás	Bekövetkezés valószínűsége	Kár			Kockázat	Védelmi intézkedés
		P	C	I	A	R	V
H1	social engineering	PVL	DD	DVL	DD	RVL	
…						4. lépés	
F1	áramszünet	PVL	-	DS	DA	RL	

Forrás: *Biztostű.hu, 2004 alapján*

4.5 Kockázatok kezelése, védelemi intézkedések számbavétele

A kockázatelemzés eddigi lépései során képet kaptunk a fenyegető veszélyforrásokról. A kockázatmenedzsment célja ennek ismeretében a kockázat hatékony csökkentése, ezáltal a biztonság növelése.

A kockázatokra adott válaszok tekintetében a nemzetközi szakirodalmak 4 fő válaszreakciót különböztetnek meg:

A *kockázatkerülés* (risk avoidance) a kockázatokat okozó tevékenységektől való elállás, vagy a kockázatokat okozó körülmények elkerülése. A kockázatelkerülés azokban az esetekben alkalmazható, amikor más kockázati válasz technikák nem használhatóak, a kockázat nem osztható meg, vagy költséghatékonyan nem lehet a kívánt kockázati szint alá csökkenteni.

A *kockázatok csökkentése* (risk reduction/mitigation) a kockázatok felismerése és azonosítása után a kockázat gyakoriságának és/vagy hatásainak csökkentésére tett lépéseket jelenti. Felöleli az IT kockázatmenedzsment eljárások megerősítését, kontrollok bevezetését.

A *kockázatmegosztás, kockázatáthárítás* (risk sharing/transfer) a kockázat gyakoriságának és/vagy hatásainak csökkentésére tett intézkedések, amely során a kockázatok megosztásra kerülnek. Eszközei lehetnek a biztosítások kötése, vagy a kockázatmegosztás a

szállítóval, külső partnerrel – outsourcing. Számos esetben a kockázat nem osztható meg vagy nem hárítható át.

A *kockázatvállalás* (risk acceptance) nem a kockázatok figyelmen kívül hagyását, hanem a tudatos kockázatvállalást jelenti, amikor bizonyos – már azonosított és dokumentált – kockázatot tudatosan felvállal a szervezet, az esetlegesen bekövetkező kárt pedig elfogadja. (ISACA, 2009, p. 28)

A fenti elméleti lehetőségek közül a kockázatkerülés a legtöbb esetben nem alkalmazható, így a kockázati tényező kezelésére alapvetően a kockázat csökkentése szolgál a megfelelő szintű védekezéssel. Bizonyos esetekben pedig a tudatos kockázatvállalás jelent megoldást.

A kockázatelemzés során feltárt veszélyekhez védelmi intézkedéseket kell rendelni. Az intézkedések kidolgozására a gyakorlatban erre vonatkozóan széleskörűen használt PreDeCo módszertant alkalmazhatjuk. A módszertan a veszélyekhez rendelt intézkedések kidolgozását, csoportosítását aszerint végzi, hogy a veszélyt megelőzni, észlelni, vagy javítani kívánjuk. A név a három fő mechanizmus angol nevének kezdetéből áll.

A módszertan a védelmet az ellenintézkedések (kontrollok) három egymásra épülő és egymást kiegészítő részre bontja:

- ✓ megelőző ellenintézkedések (**Pre**ventive):

  A megelőzés során olyan tevékenységeket kell végrehajtani, amelyek megakadályozzák, vagy csökkentik egy adott veszélyes esemény bekövetkeztét. Megelőző intézkedés lehet például az e-mail tartalomszűrés, amellyel megelőzzük a vírusok levelezésen keresztüli bejutását.
- ✓ észlelő (felismerő) ellenintézkedések (**De**tective):

  Az észlelés során a cél, hogy minél hamarabb észleljék egy adott esemény, már folyamatban lévő támadás, károkozás bekövetkeztét így korlátozva a nem kívánt hatás továbbterjedését, valamint az elhárító, helyreállító tevékenység által elősegítve annak megszüntetését.
- ✓ javító (elhárító, helyreállító) ellenintézkedések (**Co**rrective):

  A javító intézkedés célja a már megtörtént esemény által okozott kár csökkentése, a hibamentes, normál állapot minél előbbi visszaállítása. Javító intézkedés például a rendszer visszaállítása mentésből, de felkészülési tevékenységeket is jelentenek, például a biztonsági mentések elvégzése, katasztrófa elhárítási terv készítése.

A különösen nagy kárt okozó veszélyhelyzetek kezelésére külön fel kell készülni, üzletmenet folytonossági és katasztrófa-elhárítási tervek készítésével.

Figyelembe kell venni az elviselhetetlen kockázatokat is, amelyek a helyrehozhatatlan, hosszabb távon is kiható tényezők által jelentett veszélyt foglalják magukba. Ilyen kockázatok lehetnek, amikor egy veszélyforrás bekövetkezési valószínűsége kicsi, de hatása, az általa okozott kár nagyon nagy. Egy ilyen eset bekövetkezése például 10 éves időtávlatban értelmezhető, ezért az éves kockázatelemzés a védekezés nagy költsége miatt célszerűtlennek ítélheti meg a megfelelő védelmet jelentő nagy beruházást. A védelmi intézkedések kiválasztása során úgy kell kialakítani a választott megoldást, hogy az összes elviselhetetlen kockázatú veszélyforrás kockázatát legalább elviselhető mértékűvé csökkentse.

Az egyes veszélyforrásokra vonatkozóan megállapíthatóak a védelmi intézkedések, a korábbiakban alkalmazott CIA elvekhez hozzárendelhetőek a PreDeCo elvek, ezáltal előállítható a PreDeCo-CIA mátrix, amely alkalmazásával áttekintő képet kaphatunk a már feltárt kockázatok kezeléséhez kapcsolódó védelmi intézkedésekről. A táblázatot a korábban feltárt minden veszélyre kitöltve meghatározhatóak azok a védelmi intézkedések, amelyek az adott kockázat kezelésére alkalmasak. Lehetnek olyan esetek, amikor úgy ítéljük meg, hogy valamelyik típusú védelmi intézkedésre nincsen szükség, mivel az, vagy az adott sérülékenység nem értelmezhető és/vagy az adott kockázatot nem tudjuk, vagy nem kívánjuk kezelni.

9. táblázat *PreDeCo-CIA mátrix*

Veszély	**Kockázat**	**Intézkedés**	**C**	**I**	**A**
Hardver meghibásodása	Mérsékelt	**Pre**	Redundáns rendszer, megelőző karbantartás	Redundáns rendszer, megelőző karbantartás	Redundáns rendszer, megelőző karbantartás
		De	-	Integritás ellenőrző kriptográfiai eszközök	Rendszerfelügyelet működtetése
		Co	-	Biztonsági mentés	Tartalék rendszer, biztonsági mentés
Vírustámadás	Jelentős	**Pre**	Vírusszűrés, tűzfal, felhasználók oktatása	Vírusszűrés, tűzfal, felhasználók oktatása	Vírusszűrés, tűzfal, felhasználók oktatása
		De	Víruskereső	Integritás ellenőrző kriptográfiai eszközök	Rendszerfelügyelet, víruskereső
		Co	Nem védjük / biztosítás	Biztonsági mentés	Tartalék rendszer, biztonsági mentés
…	…	**…**	…	…	…

Forrás: *KIB 28. ajánlás, Tervezés az IT biztonság szempontjából*

A módszer szisztematikus alkalmazásával meghatározhatóak és dokumentálhatóak a költséghatékony, *kockázatokkal arányos* védelmi intézkedések.

A kockázatokkal arányos a védelem, ha a védelem költségei (a megfelelő időtávban) arányosak a potenciális kárértékkel. A kockázatarányos védekezés nem csak költségminimalizálás szempontjából lényeges. A biztonság fokozására tett lépések egy határon túl aránytalanul nagy költséget jelentenek, nem állnak arányban a biztonsági szint növekedésével.

A 10. táblázat a PreDeCo-CIA mátrixból – annak érdekében, hogy az eddigiekben végigvezetett „social engineering" veszélyforráshoz történő kapcsolódást is érzékeltetni lehessen – a vírustámadásra vonatkozó lehetséges védelmi intézkedéseket sorolja fel.

10. táblázat ***Védelmi intézkedések – példa vírustámadás esetén***

ID	Védelmi intézkedés	Beruházás	Éves költség	Hatás
V1	Víruskereső			
V2	Tűzfal, aktív tartalomszűrés			
V3	Felhasználók oktatása			H1/P, (valamint további, korábban azonosított veszélyforrások és a védelmi intézkedés által azokra gyakorolt hatások)
V4	Integritás ellenőrző kriptográfiai eszközök			

Forrás: *Biztostű.hu, 2004 alapján*

A védelmi intézkedések egymásra is hatással vannak. Sok esetben csak informálisan lehet az egyes hatásokat leírni. A példánál maradva a rejtjelezett levelezés bevezetése megakadályozza a tartalomszűrő tűzfal azon funkcióját, amely levelek mellékleteiből képes a vírusokat kiszűrni. A hatás oszlopban az intézkedés által befolyásolt – a kockázatelemzési táblázatban szereplő – veszélyforrás azonosítóját, valamint a befolyásolás módját szerepeltetjük. (A hatás lehet a veszélyforrás teljes kiküszöbölése (E - eliminate), az okozott kár (D – decrease damage), vagy a bekövetkezési valószínűség csökkenése (P – decrease probability).)

A kockázatelemzési táblázat korábbi példájából kiindulva, a felhasználók oktatása, a tudatosítási tevékenység csökkentheti a social engineering veszélyét is.

A fenti lépések elvégzése után készül el a kitöltött kockázatelemzési táblázat. A védelmi intézkedés oszlopába a fent megállapítottakat figyelembe véve elegendő csak a védelmi intézkedés azonosítójának feltüntetése, azonban az adott veszélyforrásra vonatkozó hatás is szerepeltethető az egyszerűbb áttekintés érdekében.

11. táblázat ***Kitöltött kockázatelemzési táblázat***

ID	Veszélyforrás	Bekövetkezés valószínűsége	Kár			Kockázat	Védelmi intézkedés
		P	C	I	A	R	V
H1	social engineering	PVL	DD	DVL	DD	RVL	V3/P
…							5. lépés
F1	áramszünet	PVL	-	DS	DA	RL	Vx/E, Vy/P

Forrás: *Biztostű.hu, 2004 alapján*

Az intézkedések kialakítása és meghozatala nem jelenti a tevékenység befejezését, az elemzést rendszeresen meg kell ismételni, és a változó körülmények, fenyegetettségek és üzemeltetési tapasztalatok alapján módosítani kell.

5 Üzletmenet-folytonosság és katasztrófatervezés

Minden olyan kockázat, amely megvalósulását az ellenintézkedések (kontrollok) nem akadályozták meg, incidensnek kell tekinteni, reagálni kell rá és kezelni kell annak érdekében, hogy ne okozzon katasztrófát. A kockázatmenedzsment sikeres eredményei közé tartozik a hatékony incidens menedzsment és a reagálási képesség.

Az elektronikus információs rendszer biztonságáért felelős vezetőnek tisztában kell lennie az üzletmenet-folytonossági terv (BCP), a katasztrófa-elhárítási terv (DRP) [15] és az incidenskezelési terv (IRP - *incident response plan*) kapcsolatával, felépítésével, azok viszonyaival. Az üzletmenet-folytonossági tervezés és a katasztrófatervezés fogalma a jegyzet korábbi fejezeteiben már megjelent. Mindkét tervnek szoros összhangban kell állnia az incidenskezelési tervvel is. Az incidenskezelési terv azokat a lépéseket tartalmazza, melyeket incidens során kell a szervezetnek megtennie.

A tervek elkészítésekor a kockázatfelmérés és a kockázatelemzés eredményeire támaszkodunk, amely során már felmértük a kritikus üzleti folyamatokat, kockázati tényezőket, azok üzleti és IT kapcsolatait.

5.1 Üzletmenet-folytonossági terv (BCP)

Az üzletmenet-folytonossági terv szerepe, hogy a szervezet – a rendkívüli helyzetekre való reagálással – akkor is fenn tudja tartani az üzletmenetet, amikor zavar keletkezik a működési feltételekben. A BCP tervekkel nemcsak a jellemző kockázatok (tűzeset, hacker-

[15] A témával részleteiben foglalkozik Rittinghouse, J. W., Ransome, J. F. (2005). Business continuity and disaster recovery for infosec managers könyv.

támadás, lopás), hanem a nem várt, illetve nehezen számszerűsíthető kockázatok (földrengés, terrortámadás) következményei is csökkenthetőek.

Az üzleti folyamatok egészét átfogó terv azokat az információkat tartalmazza, melyek alapján a támogató folyamatok (beleértve az informatikai rendszerek is) csökkenése vagy kiesése esetén miként lehet a szervezet működését fenntartani. A terv részletesen meghatározza a megelőző, helyettesítő, illetve visszaállító intézkedések (PreDeCo) megvalósításához szükséges feltételeket, szervezeti és szervezési lépéseket és a megvalósítás módját. Az elhárítás mellett a preventív, megelőző célú karbantartás csökkenti az egyes eszközök és ezáltal a teljes rendszer összeomlásának kockázatát, emellett magasabb rendszer-teljesítményt biztosít.

5.2 Katasztrófa-elhárítási terv (DRP)

A katasztrófa-elhárítás tervezés az üzletmenet-folytonosság tervezés integráns részét képezi. A tervek felépítésüket tekintve azonosak. A katasztrófaterv elkészítésének célja, hogy az előre nem látott esemény bekövetkezésekor – a rendszerek, rendszerelemek, adatok sérülésekor, kiesésekor, szélsőséges esetben megsemmisülésük esetén – hogyan állítható vissza a normál szolgáltatási szint, a rendszer, illetve az adatok. A katasztrófa azonban nem csak a rendszert, az adatokat, hanem az emberi erőforrásokat is veszélyeztetheti, így a katasztrófaterv elkészítésekor a kulcsfontosságú személyzet kérdéskörére is gondolni kell.

5.3 Incidenskezelési terv (IRP)

Az incidenskezelési és helyreállítási tervek elkészítésekor számos szempontot kell figyelembe venni, köztük a rendelkezésre álló erőforrásokat, az elvárt szolgáltatásokat, illetve, hogy milyen típusú, fajtájú és súlyosságú fenyegetésekkel néz szembe az adott szervezet. Ismerni kell az ellenőrzési szintet és az észlelési képességeket, meg kell határozni, hogy mi a szervezet által elfogadhatónak ítélt kockázati szint. A helyreállítási tervekre vonatkozó hatékony stratégia biztosítani fogja a leginkább költség-hatékony egyensúlyt a kockázatkezelés, incidens menedzsment és reagálási képesség, valamit az üzletmenet folytonosság és a katasztrófa-elhárítási tervek tekintetében.

Összefoglalás

A kockázatmenedzsment, mint az informatikai biztonság és az információbiztonság megteremtése és fenntartása érdekében szükséges tevékenység nem egyszeri, hanem folyamatos feladat rendszeres (minimum évente történő) elvégzéséről gondoskodni kell.

Az informatika biztonsági kockázatok kezelése érdekében alkalmazott kockázatelemzési módszertan az informatikai biztonsági kockázatok szisztematikus felmérését és menedzselését teszi lehetővé. A jegyzet segítséget nyújt a módszertani alapok és a hozzá kapcsolódó területekkel való összefüggéseinek bemutatásával. A kiválasztandó módszertant azonban az adott szervezet igényei szabják meg. Fontos, hogy a szervezet olyan módszert alkalmazzon, amely megfelel az igényeinek, és amely megismételhető eredményeket hoz. A módszertan csak annyit ér, amennyit a gyakorlatban megvalósítanak belőle. Ezért fontos, hogy a kockázatértékelés eredményei hasznosításra kerüljenek. Ne csak adminisztratív vagy jogszabályi kötelességből, megfelelési kényszerből készítsünk kockázatelemzést, hanem azért, mert annak eredménye a beruházási döntések és az IT menedzselési döntések miatt szükségesek.

Minden szabályzat és terv – a módszertanhoz hasonlóan – szintén annyit ér, amennyit megvalósítanak belőle. Ennek megfelelően – a kockázatelemzés alapján – a terveket aktualizálni kell és kommunikálni kell az érintettekkel.

A kockázatmenedzsment folyamatos tevékenységet jelent. A dinamikusan változó környezet, az IT és az IT biztonságot fenyegető támadási technikák folyamatos fejlődése, új rendszerek bevezetésének függvényében frissíteni szükséges a szabályzatokat, a körülményekben beálló változásoknak megfelelően újra és újra el kell végezni a kockázatelemzést és a beavatkozási tevékenységeket végre kell hajtani.

Felhasznált irodalom

21/2010. (V. 6.) IRM-MeHVM együttes rendelet a fizetési meghagyásos eljárás lefolytatásának támogatására szolgáló informatikai rendszer informatikai biztonsági követelményeiről.

77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

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

Az informatikai biztonság kézikönyve - Informatikai biztonsági tanácsadó A-tól Z-ig. Szenes, K. szerk, Verlag Dashöfer Szakkiadó, 2000-2012

Biztostű.hu (2004). Biztonság-szervezés, Forrás: http://www.biztostu.hu/course/view.php?id=15

Carr, N. G. (2003). IT Doesn't Matter. Harvard Business Review, 41-49.

Cherdantseva, Y., Hilton, J. (2014). Information Security and Information Assurance: Discussion about the Meaning, Scope, and Goals. In I. Portela, F. Almeida (Eds.) Organizational, Legal, and Technological Dimensions of Information System Administration (old.: 167-198). Hershey, PA: Information Science Reference.

Godányi, G. (2004). Katasztrófavédelem és üzletmenet folytonosság az információtechnológiában (A DR/BC tervezés alapjai). Híradástechnika, LIX. ÉVFOLYAM 2004/4, pp. 47-52.

ISACA. (2009). The Risk IT Framework. Rolling Meadows, USA.

ISACA. (2012). CISM Review Manual. ISACA.

ITB 12. számú ajánlás (1996). Informatikai rendszerek biztonsági követelményei, Budapest

KIB 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA) 1.0 verzió

KIB 25. számú ajánlása: 25/1. kötet: Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 1.0 verzió

KIB 25. számú ajánlása: 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR) 1.0 verzió

KIB 25. számú ajánlása: 25/1-2. kötet: Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió

KIB 25. számú ajánlása: 25/1-3. kötet: Az Informatikai Biztonság Irányításának Vizsgálata (IBIV) 1.0 verzió

KIB 25. számú ajánlása: 25/2. kötet: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) 1.0 verzió

KIB 25. számú ajánlása: 25/2-1. segédlet: MIBÉTS - Modell és Folyamatok 1.0 verzió

KIB 25. számú ajánlása: 25/2-2. segédlet: MIBÉTS – Útmutató a Megbízók számára 1.0 verzió

KIB 25. számú ajánlása: 25/2-3. segédlet: MIBÉTS – Útmutató a Fejlesztők számára 1.0 verzió

KIB 25. számú ajánlása: 25/2-4. segédlet: MIBÉTS – Útmutató Értékelőknek 1.0 verzió

KIB 25. számú ajánlása: 25/2-5. segédlet: MIBÉTS – Értékelési módszertan 1.0 verzió

KIB 25. számú ajánlása: 25/3. kötet: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX) 1.0 verzió

KIB 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár

Kirner, A., Pichler, A. (2007). Informatika Ellenőrzési Kézikönyv. Budapest: ISACA Hu.

Muha, L. (2007). A Magyar Köztársaság Kritikus Információs Infrastruktúráinak Védelme. PhD értekezés

Muha, L. (2008). Az információbiztonság egy lehetséges taxonómiája. Forrás: Bolyai Szemle: http://uni-nke.hu/downloads/bsz/bszemle2008/4/10_Muha_Lajos.pdf

Munk, S. (2007). Információbiztonság vs. informatikai biztonság. Forrás: Hadmérnök: http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.pdf

Munk, S. (2009). Az informatikai biztonság rendszertanához. Forrás: Bolyai Szemle: http://uni-nke.hu/downloads/bsz/bszemle2009/4/13_munksandor.pdf

Póserné, O. V. (2007): IT kockázatok, elemzésük, kezelésük Forrás: Hadmérnök: http://hadmernok.hu/archivum/2007/3/2007_3_poserne.pdf accessed April 13, 2014.

Rittinghouse, J. W., Ransome, J. F. (2005). *Business continuity and disaster recovery for infosec managers.* Elsevier Digital Press.

Secunia. (2013). Governments are Prime Targets. http://secunia.com/resources/reports/government_sector_whitepaper

Wheeler, E. (2011). Security Risk Management. Boston: Syngress.

Mellékletek

1. melléklet *ENISA kockázatmenedzsment/ kockázatelemzés módszertanok*

Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) összeállított egy, az IT-területéhez kapcsolódó kockázatmenedzsment/kockázatelemzés módszertan listát. A módszer jellemzőit leíró 21 tulajdonságot (attribútumot) tartalmazó sablon alapján elkészített leltár nem teljes, mivel nem tartalmazza az összes, az IT-hoz kapcsolódó módszert és szabványt. (Nem tartalmazza az általános menedzsment szemléletmódot képviselő (például COBIT, Basel II.) módszereket, vagy a termék- vagy rendszer-biztonság orientált módszereket, például a Common Criteria-t.)

- ✓ Austrian IT Security Handbook
- ✓ Cramm
- ✓ Dutch A&K Analysis
- ✓ Ebios
- ✓ ISAMM
- ✓ ISF Methods
- ✓ ISO/IEC 13335-2
- ✓ ISO/IEC 17799
- ✓ ISO/IEC 27001
- ✓ IT-Grundschutz
- ✓ Magerit
- ✓ Marion
- ✓ Mehari
- ✓ MIGRA
- ✓ Octave
- ✓ RiskSafe Assessment
- ✓ SP800-30

Forrás: *Inventory of Risk Management / Risk Assessment Methods (http://rm-inv.enisa.europa.eu/methods)*

2. melléklet *ENISA kockázatmenedzsment/ kockázatelemzés eszközök*

Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) összeállította a kockázatmenedzsment/kockázatelemzés területén használható eszközök listáját. A módszertanok listájához hasonlóan, ebben az esetben az eszközök jellemzőit leíró 22 tulajdonságot (attribútumot) tartalmazó sablon alapján készült a leltár. Az eszközökre vonatkozóan megerősített információkat tartalmaz a leltár, mivel vagy az adott eszköz szállítójával való kapcsolatfelvétel által megerősített, vagy közvetlenül a szállítók által beküldött adatokat tartalmazza.

- ✓ Callio
- ✓ Casis
- ✓ CCS Risk Manager
- ✓ CloudeAssurance
- ✓ Cobra
- ✓ Countermeasures
- ✓ Cramm
- ✓ EAR / PILAR
- ✓ Ebios
- ✓ GSTool
- ✓ GxSGSI
- ✓ ISAMM
- ✓ Mehari 2010 basic tool
- ✓ MIGRA Tool
- ✓ Modulo Risk Manager
- ✓ Octave
- ✓ Proteus
- ✓ Ra2
- ✓ REAL ISMS
- ✓ Resolver Ballot
- ✓ Resolver Risk
- ✓ Risicare
- ✓ Riskwatch
- ✓ RM Studio
- ✓ SISMS
- ✓ TRICK light

- ✓ Acuity Stream
- ✓ WCK

Forrás: *Inventory of Risk Management / Risk Assessment Tools (http://rm-inv.enisa.europa.eu/tools)*

„0. szint”: jelentéktelen kár

a) közvetlen anyagi kár: 10.000,- Ft-ig,
b) közvetett anyagi kár 1 embernappal állítható helyre,
c) nincs bizalomvesztés, a probléma a szervezeti egységen belül marad,
d) testi épség jelentéktelen sérülése egy-két személynél,
e) nem védett adat (nem minősített) bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.

„1. szint”: csekély kár

a) közvetlen anyagi kár: 100.000,- Ft-ig,
b) közvetett anyagi kár 1 emberhónappal állítható helyre,
c) társadalmi-politikai hatás: kínos helyzet a szervezeten belül,
d) könnyű személyi sérülés egy-két személynél,
e) „Korlátozott terjesztésű!” szolgálati titok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül,
f) személyes adatok bizalmassága vagy hitelessége sérül,
g) csekély értékű üzleti titok, vagy belső (intézményi) szabályzóval védett adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.

„2. szint”: közepes kár

a) közvetlen anyagi kár: 1.000.000,- Ft-ig,
b) közvetett anyagi kár 1 emberévvel állítható helyre,
c) társadalmi-politikai hatás: bizalomvesztés a szervezet középvezetésében, bocsánatkérést és/vagy fegyelmi intézkedést igényel,
d) több könnyű vagy egy-két súlyos személyi sérülés,
e) „Bizalmas!” szolgálati titok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül,
f) személyes adatok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül,
g) közepes értékű üzleti titok vagy egyéb jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, s a többi) védett adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.

„3. szint”: nagy kár

a) közvetlen anyagi kár: 10.000.000,- Ft-ig,
b) közvetett anyagi kár 1-10 emberévvel állítható helyre,

c) társadalmi-politikai hatás: bizalomvesztés a szervezet felső vezetésében, a középvezetésen belül személyi konzekvenciák,
d) több súlyos személyi sérülés vagy tömeges könnyű sérülés,
e) „Titkos!” szolgálati titok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül,
f) szenzitív személyes adatok, nagy tömegű személyes adat bizalmassága vagy hitelessége sérül.

„4. szint”: kiemelkedően nagy kár

a) közvetlen anyagi kár: 100.000.000,- Ft-ig,
b) közvetett anyagi kár 10-100 emberévvel állítható helyre,
c) társadalmi-politikai hatás: súlyos bizalomvesztés, a szervezet felső vezetésén belül személyi konzekvenciák,
d) egy-két személy halála vagy tömeges sérülések,
e) államtitok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül,
f) nagy tömegű szenzitív személyes adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül,
g) nagy értékű üzleti titok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.

Forrás: *IBIR 93. oldal Kárérték minta táblázat*

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.