HAJDÚDOROGI POLGÁRMESTERI HIVATAL

B09 Kockázatelemzési és -kezelési eljárást

JÓVÁHAGYÁS

Jóváhagyta:	Jóváhagyta: Czifráné dr. Urgyán Ilona
IBF	Beosztás: jegyző
Dátum:2017.10.27	Dátum:2018.05.15.
Aláírás:	Aláírás:

VÁLTOZÁSKÖVETÉS

Verzió	Dátum	Változás leírása	Módosította
3-as verzió	2017.10.27	létrehozás	Közinformatika kft. Muhr László

Tartalom

1. BEVEZETÉS

1.1. A dokumentum célja, terjedelme

Hajdúdorogi Polgármesteri Hivatal (a továbbiakban: Szervezet) bevezeti a Kockázatelemzési és -kezelési eljárást (a továbbiakban: Kockázatkezelési eljárás) a 2013 évi L. törvény, a 41/2015. (VII. 15.) BM rendelet, az ITB 8-as ajánlás, a NIST800-30 revison 1 és az ISO/IEC 27005:2012 szabvány figyelembevételével. A kockázatelemzést a 41/2015. (VII. 15.) BM rendelet szerint a Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: NEIH) által biztosított segédlet segítségével végezzük.

1.2. A dokumentum mellékletei

1. melléklet: NEIH által készített segédlet
2. melléklet: A szervezet biztonsági szintbe sorolása és a kockázatok csökkentésének érdekében javasolt védelmi intézkedések bevezetése, a maradványkockázatok elfogadásának leírása
3. melléklet: A bevezetendő védelmi intézkedések listája

2. AZ ELJÁRÁS CÉLJA, FOGALOMTÁR

Jelen Eljárás a szervezet kockázat elemzési kezelési és csökkentési alapelveit foglalja össze:

- összefoglalja a kockázatelemzés folyamatának lépéseit (kockázatfelmérés, kockázatértékelés, kockázatkezelés),
- leírja az informatikai rendszerek biztonsági osztályba sorolásának menetét és meghatározza azok szintjét,
- bemutatja, hogy a kockázatok csökkentése érdekében hogyan kell a fenyegetettségeket értékelni, illetve a védelmi intézkedéseket meghatározni, és a költésekhez képes arányos védekezést megvalósítani,

Az eljárásban a kockázatok kezelését az adatok biztonságának védendő tulajdonságai mentén vizsgálja az alábbi fő tulajdonságok alapján:

- **Bizalmasság**: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.
- **Sértetlenség**: Az adat tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. A sértetlenség fogalmába beleértendő az információk letagadhatatlansága és hitelessége is.
    - **Letagadhatatlanság:** Olyan biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az informatikai rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően.
    - **Hitelesség:** A hitelesség az entitás olyan biztonsági tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más entitás számára bizonyíthatóvá tesz.
- **Rendelkezésre állás**: Az informatikai rendszerelem – ide értve az adatot is – tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a szükséges időben és időtartamra használható.

A kockázatelemzés során külön nem elemezzük, de figyelembe vesszük az alábbi két adatbiztonsági tulajdonságokat is.

- **Elszámoltathatóság:** az entitások (például felhasználók) tevékenységeinek nyomon követhetőségét jelenti az adott entitás felelősségének megállapíthatósága érdekében.

Megbízhatóság: több mutatóval jellemzett működőképességet jelent.

A kockázatkezelés folyamata

Kockázat alatt a sebezhetőség kihasználásának negatív hatását értjük, amelyet a kihasználhatóság valószínűsége és a kihasználás hatása egyaránt befolyásol.
A **kockázatkezelés** a következő három folyamat összessége: kockázatfelmérés, kockázatértékelés és kockázatkezelés.

- **1 lépés Kockázatfelmérés:** A kockázatfelmérés során meg kell határozni az információt veszélyeztető fenyegetéseket, és azok vagyonelemekre gyakorolt hatását.
- **2. lépés Kockázatértékelés:** Az értékelés a rendszer biztonsági állapotának pontos feltérképezése a rendszer megvalósítási szakaszának végén, mely fölülvizsgálandó minden új vagyonelem vagy fenyegetés megjelenésekor, illetve törvényi vagy egyéb kötelezettségek változásakor.
- **3. lépés Kockázatkezelés:** A kockázatkezelés során az egyes feltárt kockázatokkal kapcsolatban a szervezet vezetősége dönt az alkalmazandó kockázatkezelési opcióról (elfogadás, áthárítás, csökkentés, elkerülés). A kockázatok csökkentése során olyan költséghatékony módon megvalósítható biztonsági intézkedéseket kell beépíteni a rendszerbe, melyek megfelelnek a rendszer környezetének és segítik a szervezet feladatainak teljesítését, egyúttal hozzájárulnak a korábban meghatározott kockázatok csökkentéséhez.

3. KOCKÁZATELEMZÉS

A NEIH kockázatelemzést tartalmazó támogató segédletei (Excel táblák) az eljárás mellékleteiként IER-enként megtalálhatóak, azok összesítő táblázatát az eljárás 1. melléklete tartalmazza.

3.1. A kockázat szintjének meghatározása

A kockázati szint meghatározása a bekövetkezési valószínűség és a fenyegetettség (okozott kár nagysága) osztályozásával, és azok osztályzatának mátrix szorzatával határozható meg a 2015 év 41 BM rendelet 1-3 paragrafusa és az első mellékelt egyes pontjainak irányelvei alapján.
A biztonsági osztályba sorolásnál nem a lehetséges legnagyobb kárértéket, hanem a releváns, bekövetkezési valószínűséggel korrigált fenyegetések által okozható kárt, káros hatást kell figyelembe venni.

3.2. A bekövetkezési valószínűség osztályozása

Nagyon ritka : 1

- Olyan hiba, baleset vagy környezeti katasztrófa, amely **nagyon valószínűtlen, 10 évente egyszer sem, de 100 évente egyszer vagy ritkábban** bekövetkezhet. **Jellemzően 100 évente vagy ritkábban.**

Ritka : 2

- Olyan hiba, baleset vagy környezeti katasztrófa, amely **valószínűtlen, évente egyszer sem, de 10 évente egyszer vagy többször** bekövetkezhet. **Jellemzően 10 évente.**

Átlagos : 3

- Olyan hiba, baleset vagy környezeti katasztrófa, amely **kissé valószínű, évente 1-10 alkalommal** is bekövetkezhet. **Jellemzően évente.**

Gyakori : 4

- Olyan hiba, baleset vagy környezeti katasztrófa, amely **nagyon valószínű, évente 10-100 alkalommal** is bekövetkezhet. **Jellemzően havonta.**

Nagyon gyakori: 5

- Olyan hiba, baleset vagy környezeti katasztrófa, amely **szinte bizonyosan, évente több mint 100 alkalommal** is bekövetkezhet. **Jellemzően hetente vagy sűrűbben.**

3.3. A fenyegetettség (okozott kár nagysága) osztályozása

Jelentéktelen: 1

Amennyiben a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése várhatóan jelentéktelen hátrányos hatást gyakorol a szervezet működésére, annak elemeire vagy információira. A jelentéktelen hátrányos hatás azt jelenti, hogy a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése jelentéktelen mivel:

- az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot,
- nincs bizalomvesztés, a probléma kisebb, az érintett szervezeten belül marad, és azon belül meg is oldható,
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentéktelen,
- nincs hatással az ügymenetre,
- semmilyen információ nem veszti el bizalmasságát, sértetlenségét vagy rendelkezésre állását,
- a szervezet csak minimális eszköz- vagy pénzbeli károsodást szenved általa,
- a kár pénzben kifejezhető értéke a nettó 10 000-100 000 forintot nem haladja meg,
- a kár 1 embernap vagy kevesebb munkával pótolható.

Csekély : 2

Amennyiben a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése várhatóan csekély hátrányos hatást gyakorol a szervezet működésére, annak elemeire vagy információira. A csekély hátrányos hatás azt jelenti, hogy a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése csekély mivel:

- személyes adat bizalmassága, sértetlensége, rendelkezésre állása sérülhet,
- az ügymenet szempontjából csekély értékű, és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer bizalmassága, sértetlensége, vagy rendelkezésre állása sérülhet,
- a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető,
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély,
- a működési képességet oly mértékben és olyan időtartamra csökkentheti, hogy a szervezet képes végrehajtani ugyan elsődleges funkcióit, de a funkciók hatásossága kis mértékben csökken,
- a szervezeti eszközök kisebb mértékű károsulását eredményezi, vagy
- kisebb mértékű pénzügyi veszteséget okoz, vagy
- a jogbiztonságot kisebb mértékben veszélyezteti,
- a kár pénzben kifejezhető értéke a nettó 100 000-1 000 000 forintot nem haladja meg,
- a kár 1-30 embernap munkával pótolható.

Közepes: 3

Amennyiben a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése várhatóan közepesen hátrányos hatást gyakorol a szervezet működésére, annak elemeire vagy információira. A közepesen hátrányos hatás azt jelenti, hogy a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése közepes mivel:

- különleges személyes adat, vagy nagy tömegű személyes adatok bizalmassága, sértetlensége, vagy rendelkezésre állása sérülhet,
- az ügymenet szempontjából közepes értékű, vagy az érintett szervezet szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képző adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérülhet,
- a lehetséges társadalmi-politikai hatás: bizalomvesztés az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülnek,
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest közepes,
- a működési képességet oly mértékben és olyan időtartamra csökkentheti, hogy a szervezet képes végrehajtani elsődleges funkcióit, de a funkciók hatásossága észrevehető mértékben csökken, vagy
- a szervezeti eszközök közepes károsulását eredményezi, vagy
- közepes mértékű pénzügyi veszteséget okoz, vagy
- a jogbiztonságot közepes mértékben veszélyezteti,
- a kár pénzben kifejezhető értéke a nettó 1 000 000-10 000 000 forintot nem haladja meg, vagy az érintett szervezet költségvetésének 5%-át meghaladja.
- a kár 1-12 emberhónap munkával pótolható.

Nagy: 4

Amennyiben a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése várhatóan komoly hátrányos hatást gyakorol a szervezet működésére, annak elemeire vagy információira. A komoly hátrányos hatás azt jelenti, hogy a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése nagy mivel:

- nagy tömegű különleges személyes adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérülhet,
- személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányíthatatlansága miatti veszélyeket),
- az üzlet, vagy ügymenet szempontjából nagy értékű, üzleti titkot, vagy az érintett szervezet szempontjából különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képző adat bizalmassága, sértetlensége, vagy rendelkezésre állása tömegesen, vagy jelentősen sérülhet,
- a káresemény lehetséges társadalmi-politikai hatása a bizalomvesztés a szervezeten belül, jogszabályok betartása sérülhet, bizalomvesztés az érintett szervezet felső vezetésében, az érintett szervezet vezetésében személyi konzekvenciákat kell alkalmazni,
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentős,
- a működési képességet oly mértékben és olyan időtartamra csökkentheti, hogy a szervezet képes végrehajtani elsődleges funkcióit, de a funkciók hatásossága jelentős mértékben csökken, vagy
- a szervezeti eszközök jelentős károsulását eredményezi, vagy
- jelentős pénzügyi veszteséget okoz, vagy
- a jogbiztonságot jelentős mértékben veszélyezteti,
- a kár pénzben kifejezhető értéke a nettó 10 000 000 -100 000 000 forint, vagy a költségvetési szerv vagy az érintett szervezet költségvetésének 10%-át meghaladja.

- a kár 1-10 emberév munkával pótolható.

Kiemelkedően nagy: 5

Amennyiben a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése várhatóan súlyos vagy katasztrofális hatást gyakorol a szervezet működésére, annak elemeire vagy információira. A súlyos vagy katasztrofális hátrányos hatás azt jelenti, hogy a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése kiemelkedően nagy mivel:

- kiemelten nagy tömegű különleges személyes adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül,
- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,
- a nemzeti adatvagyon helyreállítható sértetlensége nem biztosított,
- az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított,
- társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek,
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest azt meghaladóan jelentős, nagy értékű üzleti titok, az érintett szervezet szempontjából kiemelten érzékeny információt képező adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.
- a működési képességet olyan mértékben és olyan időtartamra csökkentheti, illetve akár meg is szüntetheti, hogy a szervezet nem képes végrehajtani egy vagy több elsődleges funkcióját, vagy
- a szervezeti eszközök lényegi súlyos anyagi hatással járó károsulását eredményezi, vagy
- lényegi pénzügyi veszteséget okoz, vagy
- a jogbiztonságot alapvető mértékben veszélyezteti,
- a kár pénzben kifejezhető értéke a nettó 100 000 000 forintot meghaladja, vagy az érintett szervezet költségvetésének 15%-át meghaladja.
- a kár több mit 10 emberév munkával pótolható.

3.4. Biztonsági osztályok

A szervezet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény és a 2015. évi 41. BM rendelet valamit az ITB 8-adik ajánlása által adott szempontok figyelembevételével az alábbiak szerint hozta létre a biztonsági osztályokat:

Az 1. biztonsági osztály esetében csak jelentéktelen káresemény következhet be, mivel

- az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot;
- nincs bizalomvesztés, a probléma kisebb, az érintett szervezeten belül marad, és azon belül meg is oldható;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentéktelen.

A 2. biztonsági osztály esetében csekély káresemény következhet be, mivel

- személyes adat sérülhet;
- az ügymenet szempontjából csekély értékű és/vagy csak belső (intézményi) szabályzóval védett adat, vagy elektronikus információs rendszer sérülhet;
- a lehetséges társadalmi-politikai hatás az érintett szervezeten belül kezelhető;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély.

A 3. biztonsági osztály esetében közepes káresemény következhet be, mivel

- különleges személyes adat vagy nagy tömegű személyes adatok sérülhetnek;
- az ügymenet szempontjából közepes értékű, vagy az érintett szervezet szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett adat sérülhet;
- lehetséges társadalmi-politikai hatás: bizalomvesztés állhat elő az érintett szervezeten belül, vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest közepes.

A 4. biztonsági osztály esetében nagy káresemény következhet be, mivel

- nagy tömegű különleges személyes adat sérülhet;
- személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket);
- az ügymenet szempontjából nagy értékű, üzleti titkot, vagy az érintett szervezet szempontjából különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen vagy jelentősen sérülhet;
- a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, az érintett szervezet vezetésében személyi konzekvenciákat kell alkalmazni;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentős.

Az 5. biztonsági osztály esetében kiemelkedően nagy káresemény következhet be, mivel

- kiemelten nagy tömegű különleges személyes adat sérül;

- emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be;
- a nemzeti adatvagyon helyreállíthatatlanul megsérülhet;
- az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított;
- a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek;
- a közvetlen és közvetett anyagi kár az érintett szervezet költségvetését, szellemi és anyagi erőforrásait meghaladó, különösen nagy értékű üzleti titok, az érintett szervezet szempontjából kiemelten érzékeny információt képező adat sérül.

3.5. A biztonsági osztály meghatározása

A biztonsági osztály meghatározása az alábbi mátrix alapján történik, ahol a **káresemények nagyságát** 1-től 5i-g osztályozzuk:

- Jelentéktelen: 1
- Csekély : 2
- Közepes: 3
- Nagy: 4
- Kiemelkedően nagy: 5

A **bekövetkezés gyakoriságot** 1-5ig osztályozzuk:

- Nagyon ritka: 1
- Ritka: 2
- Átlagos: 3
- Gyakori: 4
- Nagyon gyakori: 5

A **biztonsági osztályt** pedig a káresemény nagyságának a bekövetkezési gyakorisággal kombinált mátrixa alapján a következőképpen határozzuk meg.

1. biztonsági osztály:	1
2. biztonsági osztály:	2
3. biztonsági osztály:	3
4. biztonsági osztály:	4
5. biztonsági osztály:	5

A kockázatokat a B09-1 kockázatkezelési v3.1.xls alapján kell elvégezni. ahol a bekövetkezés gyakoriságának és a káresemény nagyságának szorzata alapján kell a kockázatoka kezelni. Minden 12 pontnál nagyobb kockázat kezelendő, az alatt lévő kockázattal bíró fenyegetések elvállalhatók, azok monitorozása mellett.

A káresemény nagyságának a bekövetkezési gyakorisággal kombinált szorzata					
Bekövetkezési gyakoriság:	**Káresemény nagysága**				
	1. Jelentéktelen káresemény következhet be:	**2.** Csekély káresemény következhet be.	**3.** Közepes káresemény következhet be.	**4.** Nagy káresemény következhet be.	**5.** Kiemelkedően nagy káresemény következhet be.
5. Nagyon gyakori	**5**	**10**	**15**	**20**	**25**
4. Gyakori	**4**	**8**	**12**	**16**	**20**
3. Átlagos	**3**	**6**	**9**	**12**	**15**
2. Ritka	**2**	**4**	**6**	**8**	**10**
1. Nagyon ritka	**1**	**2**	**3**	**4**	**5**

Biztonsági osztály besorolása

A káresemény nagyságának a bekövetkezési gyakorisággal kombinált biztonsági osztálya					
Bekövetkezési gyakoriság:	**Káresemény nagysága**				
	1. Jelentéktelen káresemény következhet be:	**2.** Csekély káresemény következhet be.	**3.** Közepes káresemény következhet be.	**4.** Nagy káresemény következhet be.	**5.** Kiemelkedően nagy káresemény következhet be.
5. Nagyon gyakori	**1**	**2**	**3**	**4**	**5**
4. Gyakori	**1**	**2**	**3**	**4**	**5**
3. Átlagos	**1**	**2**	**3**	**4**	**4**
2. Ritka	**1**	**2**	**3**	**3**	**3**
1. Nagyon ritka	**1**	**1**	**1**	**2**	**2**

Lásd: NIST 800-30 revision 1.: TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

A mátrix alapján kapott biztonsági osztályokat a 2015. BM 41. rendelet értelmében, a kockázatelemzés során módosíthatjuk; védelmi intézkedések bevezetésével és a kockázatok kezelésével magasabb vagy alacsonyabb biztonsági osztályba sorolhatjuk a rendszert.

3.6. Kockázatok kezelése

A kockázatok elemzését a B09-1 Kockázatok elemzése táblázaton kell elvégezni. Amelynek az eredményei alapján kell meghatározni a szervezet:
Biztonsági szintjét,
Biztonsági osztályát,
Az elfogadható a kezelendő, és a nem elfogadható és az azonnali cselekvést igénylő kockázatokat.

A B09-1 Kockázatok elemzése táblázat, Kockázatok értékelése táblán összegzi a felárt kockázatokat és a javasolt védelmi intézkedéseket, amelyek elfogadásra kerülnek a szervezet vezetése által és bekerülnek a szervezet B05 Információbiztonsági stratégiába.

A kockázatkezelés során az egyes feltárt kockázatokkal kapcsolatban a szervezet vezetősége dönt az alkalmazandó kockázatkezelési opcióról (elfogadás, áthárítás, csökkentés, elkerülés). A kockázatok csökkentése során olyan költséghatékony módon megvalósítható biztonsági intézkedéseket kell beépíteni a rendszerbe, melyek megfelelnek a rendszer környezetének és segítik a szervezet feladatainak teljesítését, egyúttal hozzájárulnak a korábban meghatározott kockázatok csökkentéséhez.

3.7. A kockázatok kezelésének módjai

A kockázatkezelési intézkedések célja a biztonsági kockázatoknak az elfogadható/méltányos költségen történő azonosítása, kézbentartása, minimalizálása vagy megszüntetése, amelyek hatással lehetnek az információs rendszerekre.
A kockázatkezelés során a feltárt kockázatok kezelési lehetőségeit jelen eljárás és annak biztonsági tervei tartalmazzák. A kockázatkezelés során a kockázatkezelési, kockázatcsökkentési lehetőségeket alkalmazhatjuk, úgymint:

- megfelelő biztonsági intézkedések alkalmazása a kockázatok csökkentése érdekében;
- a kockázatok tudatos, objektív felvállalása, elfogadása;
- a kockázatok elkerülése úgy, hogy a szervezet nem használja azokat a szolgáltatásokat, vagy eljárásokat, ahol az adott kockázatok előfordulnak;
- a kockázatok áthárítása úgy, hogy a szervezet számára kockázatos szolgáltatásokkal, eljárásokkal kapcsolatos veszélyeket áthárítjuk külső szereplőkre, pl. biztosítókra vagy beszállítókra;
- a kockázatok megosztása.

3.8. A kockázatok csökkentésének módjai

A kockázatok csökkentése érdekében a szervezetnek az alábbi csoportokba sorolható biztonsági intézkedéseket kell megtennie a 41/2015. (VII. 15.) BM rendelet 3. és 4. melléklete szerinti védelmi intézkedések bevezetésével.

3.8.1. Adminisztratív védelmi intézkedések

- **Adminisztratív védelmi intézkedések** előírások, szabályzatok formájában, melyek betartása elemzéssel, oktatással, képzéssel, illetve szankcionálással érhető el. Az adminisztratív intézkedések célja – többek között – az összes védelmi intézkedés egységbe foglalása is.
- **Menedzsmentbiztonsági intézkedések**, melyek a kockázatok és az informatikai rendszerek biztonságának menedzselésére koncentrálnak (pl. kockázatfelmérés, rendszer- és szolgáltatás-beszerzés, biztonság-értékelés és auditálás);

3.8.2. Fizikai védelmi intézkedések

- **Fizikai védelmi intézkedések**, melyek az informatikai eszközök fizikai védelmét szolgálják.

3.8.3. Logikai védelmi intézkedések

- **Üzemeltetési biztonsági intézkedések**, melyeket elsősorban emberek valósítanak meg, hajtanak végre (pl. fizikai és környezeti védelem, személyzethez kapcsolódó biztonság, képzés, konfigurációkezelés, működés-folytonosság, adathordozók kezelése);
- **Műszaki biztonsági intézkedések**, melyeket elsősorban az informatikai rendszer valósít meg, hajt végre, a rendszer hardver, szoftver összetevőiben megvalósuló mechanizmusok segítségével (pl. azonosítás, hitelesítés, naplózás, rendszer- és kommunikációvédelem, biztonsági incidensek kezelése).
- **Algoritmikus védelmi intézkedések**, ahol a védelem az informatika eszközeivel (algoritmusokkal) megoldható, pl. ide tartoznak a titkosítási, vírusvédelmi, hálózati forgalomszűrési intézkedések;

3.9. Védelmi intézkedés típusai

A védelmi intézkedés aszerint, hogy a fenyegetettséget, veszélyt megelőzni, észlelni vagy javítani kíván vagy szankciókat helyez kilátásba, vagy alkalmaz az alábbi típusúak lehetnek:

- **Megakadályozó, megelőző (preventív):** a megelőzés során olyan tevékenységeket kell végrehajtani, amely lehetetlenné teszi a veszélyes esemény bekövetkeztét. Megelőző intézkedés például e-mail tartalomszűrés, amellyel megelőzzük vírusok levelezésen keresztüli bejutását.
- **Észlelő (detektáló):** az észlelés során a már folyamatban lévő támadást, károkozást próbáljuk – lehetőleg minél hamarabb – észlelni, majd ez alapján megszüntetni, mielőtt lényegi károkozásra kerülne sor. Ilyen például a behatolásjelző (IDS) rendszer használata, amely gyanús hálózati forgalom esetén riasztást ad. Az észlelés alapján azután más tevékenységeket is végezhetünk.
- **Helyreállító (korrektív):** a helyreállító intézkedés a már megtörtént esemény által okozott kárt csökkenti, vagy szünteti meg. Javító intézkedés például a rendszer visszaállítása mentésből, de ilyen intézkedés akár az is, ha biztosítással rendelkezünk, amely kár esetén biztosít fedezetet.
- **Fegyelmi (deterrent):** a fegyelmi intézkedések belső eljárási rendje szerint fegyelmi eljárást kezdeményez vagy helyez kilátásba az elektronikus információ biztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben, vagy előre rögzíti a nem

elfogadott viselkedést és cselekedeteket. Amennyiben az elektronikus információ biztonsági szabályokat nem az érintett szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.

4. ÉRTÉKELÉS ÉS FELÜLVIZSGÁLAT

A szervezet belső működését támogató rendszerek és szolgáltatások köre – összhangban az Információbiztonsági stratégiában foglaltakkal – folyamatosan bővül. Ennek támogatása érdekében a támogató informatikai rendszerek technológiai és funkcionális oldalról egyaránt fejlődnek, amelyek új kockázatokat, fenyegetettségeket jelentenek a szervezet működésére.
A kockázatok, fenyegetettségek kezelésére az Iskolának az informatikai rendszerek informatikai biztonsági kockázatait legalább éves rendszerességgel fel kell mérnie, és gondoskodnia az informatikai célrendszer kockázatokkal arányos védelméről a tervezés, a beszerzés, az előállítás, az üzemeltetés és a felülvizsgálat területén. Az évenkénti felülvizsgálatot sűríteni kell

- valamely informatikai célrendszer működésének jelentős változása esetén,
- új informatikai célrendszer bevezetésekor,
- a célrendszereket támogató infrastruktúra (szerverek, hálózat, stb.) jelentős változása esetén,
- törvényi vagy egyéb változások esetén,
- jelentősebb incidens után (az incidens kivizsgálását követően).

Az értékelés és felülvizsgálat eredményeit dokumentálni kell, annak megfelelően aktualizálni kell a jelen Eljárást.

5. AZ INFORMATIKAI RENDSZER ELEMEINEK CSOPORTOSÍTÁSA, AZOK GYENGE PONTJAI ÉS FENYEGETŐ TÉNYEZŐI

Az Informatikai Tárcaközi Bizottság az ITB 8-as ajánlásában rögzíti, az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemeit a biztonsági szempontok és védelmi intézkedések célirányos kezelhetősége érdekében meghatározott orientációjú csoportokba sorolja. Ennek a csoportosításnak a figyelembevételével egyszerűsödik a már meglévő és az alkalmazni kívánt újabb rendszerelemeknek, azok különös gondosságot igénylő gyenge pontjainak, valamint az elsősorban a gyenge pontokra ható fenyegető tényezőknek feltérképezése, kapcsolataik meghatározása.

Az ITB 8-as ajánlás 3. fejezetében az alábbi elemcsoportokat és az azokhoz tartozó gyengeségeket és fenyegetettségeket alakította ki:
a) a környezeti infrastruktúra elemei,
b) a hardver elemek,
c) az adathordozók,
d) a dokumentumok,
e) a szoftver elemek,
f) az adatok,
g) a kommunikáció elemei,
h) a rendszerelemekkel kapcsolatba kerülő személyek.

A felsorolást lásd az ITB 8 ajánlás 3.3 fejezetében!

6. A SZERVEZET INFORMATIKAI RENDSZEREINEK BIZTONSÁGI SZINTBE SOROLÁSA

A szervezet informatikai rendszereinek mindenkori biztonsági szintbe sorolását a NEIH által készített segédlet alapján az 1. melléklet összefoglalva tartalmazza, amelyből a biztonsági szintbe sorolás indoklását és a kockázatok elfogadását a 2. melléklet tartalmazza.

7. A SZERVEZET VÉDELMI INTÉZKEDÉSEI

A szervezet informatikai rendszerének szintbesorolása alapján a 3. melléklet tartalmazza a bevezetendő védelmi intézkedések listáját.

Hajdúdorog 2018. 05.15.

Czifráné dr. Urgyán Ilona
jegyző