INNOVÁCIÓS ÉS TECHNOLÓGIAI
MINISZTÉRIUM

ÚTMUTATÓ A KIBERVÉDELMI KOCKÁZATÉRTÉKELÉS ELKÉSZÍTÉSÉHEZ

2022.

Jelen dokumentum az Útmutató a kibervédelmi kockázatértékelés elkészítéséhez témakörben készült el.

Budapest, 2022.03.08.

Innovációs és Technológiai Minisztérium * 166. *

Dr. Löwinger Máté
főosztályvezető

Készítette:
Innovációs és Technológiai Minisztérium
Közlekedéspolitikáért Felelős Államtitkárság
Közlekedési Hatósági Ügyekért Felelős Helyettes Államtitkárság
Légügyi Kockázatértékelési Hatósági Főosztály
Érvényes: 2022.03.08-tól

Tartalom

1. Bevezető

1.1. Az útmutató célkitűzései

Az *Útmutató a kibervédelmi kockázatértékelés elkészítéséhez* (a továbbiakban: Útmutató) azzal a céllal íródott, hogy eljárási segédletként szolgáljon a vonatkozó jogszabályok által meghatározott kibervédelmi előírások értelmezése és alkalmazása során az 1995. évi XCVII. törvény 1. § (1) és (2) bekezdésének hatálya alá tartozó és a légiközlekedés védelmében érintett szervezetek számára.
Az Útmutató logikai sorrendben lépésről-lépésre végighalad a kockázatértékelési feladatok elkészítési szakaszain.

1.2. Vonatkozó jogszabályi követelmények

- A közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról szóló 2015/1998/EU rendelet mellékletének 1.7. pontja;
- A polgári légiközlekedés védelmének szabályairól és a Légiközlekedési Védelmi Bizottság jogköréről, feladatairól és működési rendjéről szóló 169/2010. Kormányrendelet 40/A. §-a.

2. Kockázatértékelés

A kockázatértékelés célja a szervezet működését veszélyeztető események kockázatainak azonosítása, ezek bekövetkezési valószínűségének értékelése, az arányos és hatásos védekezés, megelőzés módjának és mértékének kidolgozása, valamint a felelősségek leosztása. A kockázatértékelés során a feltárt védelmi és biztonsági kockázatok elemzésének eredményét fontos az érintett szervezeti alegységek dolgozóival megismertetni, hogy kialakítható és alkalmazható legyen a kockázattal arányos védekezés.

Az átfogó kockázatértékelés elkészítése az alábbi táblázat segítségével történik, melynek kitöltéséhez a következő alfejezetek nyújtanak segítséget:

Kockázati tényező	Kockázati érték	Kockázatcsökkentő intézkedések	Felelős személy

2.1. Kockázati tényező

A szervezet profilja, működési elvei, fizikai kialakítása nagymértékben befolyásolja az alkalmazandó kibervédelmi intézkedések szintjét és mértékét.
A kockázati események azonosítása során elsősorban a kibertámadás potenciális célpontjait a 169/2010. (V. 11.) Korm. rendelet 40/A § (3) (4), valamint (8) bekezdésére tekintettel kell számba venni az adott szervezet vonatkozásában, beleértve az informatikai rendszereket és a tárolt, felhasznált vagy továbbított adatokat, illetve az összes olyan rendszerelemet, mely a kibertámadások tárgyává válhatnak. Ezután az azonosított célpontokra irányuló potenciális veszélyek és kibervédelmi események azonosítása ajánlott.

2.1.1. Kritikus rendszerelemek azonosítása

A kockázatértékelés megkezdéséhez azonosítani kell a szervezet működése során használt, a kibervédelem szempontjából kritikus adatokat és információs rendszereket, szoftvereket és hardvereket, melyek vonzó célpontok lehetnek a potenciális elkövetők számára. A hálózati és információs rendszerek védelme magában foglalja a tárolt, továbbított és kezelt adatok védelmét. Ajánlott egy átfogó felmérést készíteni a lehetséges célpontokról, figyelembe véve azok kritikusságát a szervezet működése szempontjából:

a. a repülés védelme és biztonsága szempontjából kritikusnak minősített rendszerek és adatok (pl.: légiforgalmi irányítási rendszerek, indulás-ellenőrzési rendszerek, a légijármű kommunikációs, navigációs és biztonság szempontjából kritikus rendszerei, légijármű-irányító és diszpécserszolgálatok);
b. repülésvédelmi szempontból kritikus rendszerek és adatok (a meghatalmazott ügynökök, ismert szállítók, meghatalmazott beszállítók adatbázisa, beléptető rendszerek, kártyaleolvasók, kamerás megfigyelőrendszerek, utas és poggyász összeegyeztető rendszer, a védelmi átvizsgálásra használt rendszerek és robbanóanyag felderítő rendszerek, a repülőtéri azonosító kártya adatbázis, a foglalkoztatásra és a védelmi háttérellenőrzésre vonatkozó adatbázis, a személyek védelmi képzésére vonatkozó adatbázis);

c. a légiközlekedés könnyítése szempontjából kritikusnak minősített rendszerek és adatok (pl.: helyfoglalási és utasfelvételi rendszerek, információs kijelző rendszerek, poggyászkezelő rendszerek, határátkelő- és vámrendszerek).

A kibervédelmi kockázatértékelés során ugyanakkor javasolt figyelembe venni a felhasználói jogosultságok adminisztrációját, a hozzáférési szintek kialakítását, az egyedi jogosultságokat, ezek engedélyezését, a felelősségi körök meghatározását, melyek szintén fontos támadási felületet biztosíthatnak.

2.1.2. A jogellenes beavatkozások azonosítása

A kibertámadási kockázati tényezők meghatározása során a lehetséges jogellenes beavatkozásokat és támadásokat, a már azonosított kritikus rendszerelemeket potenciálisan fenyegető külső és belső kockázatok azonosítását javasolt elvégezni, amely magában foglalja a támadás módját, módszereit és a támadó személyét. Javasolt azonosítani az ismert szereplőket, ideértve a hackereket, bűnszervezeteket, bennfenteseket, figyelembe véve azok motivációját (pl. anyagi haszonszerzés, működés megzavarása, gazdasági érdek, kizsákmányolás), a rendelkezésre álló erőforrásokat és felkészültségüket.
Ennek kellően részletesnek kell lennie ahhoz, hogy lehetővé tegye a pontos értékelést és elemzést.

2.2. Kockázati érték

A kockázati értéket az adott kockázatnak a szervezet működésre gyakorolt hatása és annak bekövetkezési valószínűsége adja az alábbi táblázat szerint:

		A működésre gyakorolt hatás				
		nagyon alacsony	alacsony	közepes	magas	nagyon magas
A bekövetkezés valószínűsége	nagyon magas	**5A**	**5B**	**5C**	**5D**	**5E**
	magas	**4A**	**4B**	**4C**	**4D**	**4E**
	közepes	**3A**	**3B**	**3C**	**3D**	**3E**
	alacsony	**2A**	**2B**	**2C**	**2D**	**2E**
	nagyon alacsony	**1A**	**1B**	**1C**	**1D**	**1E**

A kapott kockázati érték függvényében további intézkedések bevezetése válhat szükségessé az alábbiak szerint:

- zöld – elfogadható szintű kockázat, intézkedést nem igényel
- sárga – elfogadható, megfelelő kockázatcsökkentő intézkedések mellett,
- piros – nem elfogadható, sürgős intézkedés szükséges.

2.2.1. A támadás bekövetkezésének valószínűsége

Az elkövető szándékát és képességét figyelembe véve a támadás valószínűsége lehet:

1 - nagyon alacsony: elméletileg valószínű a támadás előfordulása, de annak tervezésére konkrét jelek nincsenek.
2 - alacsony: nincs közelmúltbeli példa a támadásra, de vannak a szándékra utaló jelek, azonban a módszer láthatóan nem kellően kidolgozott annak sikeres végrehajtásához
3 - közepes: valószínű kibervédelmi támadás, a szándék és képesség némi bizonyítékával, esetleg néhány példával, de nincs bizonyíték a jelenlegi támadástervezésre
4 - magas: nagyon valószínű a támadás előfordulása, viszonylag friss példák vagy bizonyítékok vannak hasonló támadásokra
5 - nagyon magas: nagyon valószínű kibervédelmi esemény, amikor egy ilyen jellegű tényleges támadás történt a közelmúltban, vagy erős jelek utalnak a képesség, szándék és tervezés lehetőségére.

2.2.2. A támadás szervezetre gyakorolt hatása

Az adott támadás következményeinek természete és mértéke, a lehetséges gazdasági, politikai, reputációs veszteségek mértéke:

A - nagyon alacsony: a szervezetre minimális hatást fejt ki, kritikus szervezeti egységeket nem érint, a károk minimális erőfeszítéssel csökkenthetők
B - alacsony: viszonylag kis károkat okozhat, melyek nagyon kis mértékben befolyásolják a szervezet működését
C - közepes: kezelhető mértékű károkat okozna, a szervezet működését mérsékelten érintheti, de a veszteségek kezelhetőek
D - magas: nagy károkat, részleges leállást okozhat
E - nagyon magas: gyakorlatilag megbénítaná a szervezet működését, felbecsülhetetlen károkat okozna.

2.3. Kockázatcsökkentő intézkedések

A kibertámadások kockázatának kezelhető szinten tartása érdekében bevezetett megelőző és/vagy kockázatcsökkentő intézkedések részletes meghatározása javasolt. Kockázatértékelés alapján a légiközlekedésben alkalmazott összes létfontosságú rendszer és adat védelmét már a tervezési szakaszban indokolt megkezdeni, hogy azok a megfelelő szintű ellenálló képességet biztosítsanak a kibertámadásokkal szemben.
Ugyanakkor a fejlesztési és karbantartási munkák során, illetve a teljes felhasználási és megsemmisítési ciklus alatt is szem előtt kell tartani a kibervédelmi megfontolásokat. Az adattárolási eljárásoknak összhangját javasolt biztosítani a mindenkor érvényes adatkezelési szabályozások követelményeivel, amelyek az adatok minősítése szerint írja elő a szükséges védelmi szintet, a megfelelő őrzési időt és a megsemmisítési módszereket.
A kibervédelmi kockázatkezelési terv fontos eleme a kockázati szint csökkentése érdekében végrehajtott folyamatos felülvizsgálat, mely során meghatározott időnként a szervezet visszaellenőrzi saját eljárásait.

2.4. Felelős személy

A kockázat „tulajdonosa" az, akinek felelőssége az adott kockázat értékelése és kezelése, illetve a kockázatcsökkentő intézkedések bevezetése és azok alkalmazásának vagy fenntartásának kezelése.