Biztonsági eseménykezelés és üzletmenet-folytonosság – az egyes szabályozási területek eltérő hatóköre és kapcsolódása

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/33

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.08.28	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Jelen állásfoglalás célja, hogy elhatárolja egymástól a biztonsági eseménykezelés (incidenskezelés) és az üzletmenet-folytonosság szabályozási területét, bemutassa a két terület eltérő hatókörét a Kiberbiztonsági tv. és végrehajtási rendeletei alapján, valamint rögzítse, hogy a NIS2 felkészülés és a kiberbiztonsági audit során a két területet hol és hogyan kell összekapcsolni.

A két terület kiindulópontja és célja eltér. A biztonsági eseménykezelés reaktív és eseményvezérelt: egy konkrét kiberbiztonsági incidens (vagy annak gyanúja) váltja ki, célja az incidens észlelése, elemzése, elszigetelése, felszámolása és a hatósági bejelentési kötelezettségek határidőben történő teljesítése. Az üzletmenet-folytonosság ezzel szemben megelőző és rendelkezésre állás-központú: attól függetlenül működik, hogy a kiesést kibertámadás, üzemzavar, emberi hiba vagy természeti esemény okozza, célja pedig az, hogy a szervezet alapfeladatai és alapfunkciói a kiesés ellenére is előre meghatározott szinten és időn belül működjenek, illetve helyreálljanak.

A hatókörök közötti legfontosabb gyakorlati különbség, hogy a biztonsági eseménykezeléshez kötelező, szigorú határidőkhöz kötött hatósági bejelentési rezsim tartozik (első bejelentés 24 órán, eseménybejelentés 72 órán belül, zárójelentés egy hónapon belül), míg az üzletmenet-folytonosság elsődlegesen belső, tervezési és tesztelési kötelezettségeket keletkeztet (üzletmenet-folytonossági szabályzat és terv, mentések, tartalék helyszínek, rendszeres tesztelés), amelyek teljesülését a kiberbiztonsági audit ellenőrzi.

A két terület ugyanakkor nem választható el élesen, az incidenskezelés törvényi fogalma maga is magában foglalja az incidenst követő helyreállítást, a 7/2024. (VI. 24.) MK rendelet pedig mindkét irányból kifejezetten előírja a két terület összehangolását. Az auditra való felkészülés során ezért nem elegendő a két tervdokumentum önálló megléte, igazolni kell az eszkalációs pontokat, a közös tesztelést és a helyreállítási célok (RTO, RPO) összhangját is.

2. A VIZSGÁLANDÓ KÉRDÉS

Miben tér el egymástól a biztonsági eseménykezelés és az üzletmenet-folytonosság szabályozási hatóköre a magyar NIS2 szabályozásban, és hogyan kapcsolódik egymáshoz a két terület?

3. VÁLASZ

3.1 Fogalmi behatárolás

3.1.1 Esemény, kiberbiztonsági incidens és incidenskezelés

A biztonsági eseménykezelés fogalmi alapjait a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) értelmező rendelkezései adják. A

törvény különbséget tesz a semleges „esemény” és a védelmi célokat ténylegesen veszélyeztető „kiberbiztonsági incidens” között.

> *„27. esemény: az elektronikus információs rendszerben bekövetkezett állapotváltozás;” [2024. évi LXIX. törvény 4. § 27. pont]*
> *„46. kiberbiztonsági incidens: olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;” [2024. évi LXIX. törvény 4. § 46. pont]*

Az incidenskezelés törvényi fogalma a teljes életciklust lefedi, a megelőzéstől a működés helyreállításáig, illetve nem kifejezetten minden tárolt, kezelt adatra vonatkozik akkor is ha az laptop vagy pendrive vagy egy nyomtató memóriája. Ez a definíció a két vizsgált terület kapcsolódása szempontjából kulcsfontosságú, mert az incidenskezelés szükségszerűen „belenyúlik” az üzletmenet-folytonosság területébe.

> *„47. kiberbiztonsági incidenskezelés: minden olyan tevékenység és eljárás, amelynek célja a kiberbiztonsági incidens megelőzése, észlelése, elemzése és elszigetelése vagy a kiberbiztonsági incidensre való reagálás és a kiberbiztonsági incidenst követően a működés helyreállítása;” [2024. évi LXIX. törvény 4. § 47. pont]*

A bejelentési kötelezettség szempontjából a „jelentős kiberbiztonsági incidens” fogalmának van kiemelt jelentősége. A törvény többek között a szolgáltatás vagy az éves bevétel legalább 5%-os kiesésével járó vagy fenyegető, illetve súlyos működési zavart, pénzügyi vagy reputációs veszteséget okozó vagy okozni képes incidenst minősíti jelentősnek.

> *„a) a közvetlenül alkalmazandó európai uniós jogi aktusban ekként meghatározott kiberbiztonsági incidens,*
> *b) közvetlenül alkalmazandó európai uniós jogi aktus hiányában az olyan kiberbiztonsági incidens, amely*
> *ba) a szervezet üzleti szolgáltatásának vagy a szervezet által nyújtott szolgáltatásnak legalább 5%-os csökkenésével vagy a szervezet éves bevételének legalább 5%-os kiesésével jár vagy fenyeget;*
> *bb) súlyos működési zavart okoz vagy képes okozni a szolgáltatásokban, vagy pénzügyi vagy reputációs veszteséget okoz vagy képes okozni a kiberbiztonsági incidens által érintett szervezetnek vagy személynek; vagy*
> *bc) jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett, vagy képes érinteni;”*

Megjegyzendő, hogy az üzletmenet-folytonossági tervezés során képzett üzleti hatáselemzési adatok (kiesési szintek, bevételi hatás) közvetlenül felhasználhatók annak megítéléséhez, hogy egy incidens eléri-e a jelentős incidens küszöbét.

3.1.2 Az üzletmenet-folytonosság fogalmi helye

Az „üzletmenet-folytonosság” kifejezésre a Kiberbiztonsági tv. önálló definíciót nem tartalmaz, de definiálható a következőként: „egy vállalat azon képessége, hogy előre meghatározott és elfogadható szinten **folytassa a termelést vagy a szolgáltatást** egy kárt okozó, váratlan eseményt követően.” A terület jogi tartalmát egyrészt a törvény alapelvi szintű követelménye – a zárt, teljes körű, folytonos és a kockázatokkal arányos védelem, valamint a rendelkezésre állás biztosítása [2024. évi LXIX. törvény 4. § 84. és 99. pont, 5. § (1) bekezdés] –, másrészt a biztonsági osztályba sorolás követelményeiről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: MK rendelet) 2. mellékletének 7. fejezete (készenléti tervezés, üzletmenet-folytonosság) tölti ki. Ez az elhatárolás megfelel a NIS2 irányelv [(EU) 2022/2555 irányelv] logikájának is, amely a 21. cikk (2) bekezdésében az eseménykezelést (b) pont) és az üzletmenet-folytonosságot – ideértve a biztonsági mentések kezelését, a katasztrófa utáni helyreállítást és a válságkezelést (c) pont) – két önálló, de egymás mellett kötelező kockázatkezelési intézkedésként nevesíti.

A definícióból jól látszik, hogy az üzletmenet folytonosság terület a szervezet folyamatos működésének fenntartására fókuszál, tehát egy adatszivárgás nem tartozik ide, ugyanakkor akár súlyos incidens is lehet.

3.2 A biztonsági eseménykezelés szabályozási hatóköre

A biztonsági eseménykezelés hatóköre három szabályozási szinten ragadható meg: a szervezet vezetőjének törvényi kötelezettségei, az MK rendelet szerinti védelmi intézkedések, valamint a hatósági bejelentési rezsim szintjén.

3.2.1 A szervezet vezetőjének törvényi kötelezettségei

A Kiberbiztonsági tv. a szervezet vezetőjének közvetlen felelősségévé teszi az incidensekre való gyors és hatékony reagálást, a bejelentést és a helyreállítást.

> *„e) az elektronikus információs rendszert érintő kiberfenyegetés, kiberbiztonsági incidensközeli helyzet vagy kiberbiztonsági incidens bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a gyors és hatékony reagálásról, az illetékes kiberbiztonsági incidenskezelő központnak való bejelentésről, a kiberbiztonsági incidensek kezeléséről, valamint a helyreállításról;” [2024. évi LXIX. törvény 6. § (5) bekezdés e) pont]*
> *„f) gondoskodik az érintetteknek a kiberbiztonsági incidensekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáról;” [2024. évi LXIX. törvény 6. § (5) bekezdés f) pont]*

Figyelemre méltó, hogy a törvényi kötelezettség már ezen a szinten is tartalmazza a helyreállítást, vagyis az eseménykezelés törvényi hatóköre az incidens lezárásáig, a működés visszaállításáig terjed.

3.2.2 Védelmi intézkedések: az MK rendelet 2. mellékletének 9. fejezete

Az MK rendelet 2. mellékletének 9. fejezete (biztonsági események kezelése) határozza meg az auditon számon kérhető konkrét kontrollokat. A szervezetnek már „alap” biztonsági osztályban

is rendelkeznie kell biztonsági eseménykezelési szabályzattal és eljárásrenddel, valamint kiépített eseménykezelési képességgel.

> *„9.9.2. Biztonsági eseménykezelési képességet alakít ki, amely összhangban van a biztonsági eseménykezelési tervvel, és magában foglalja a felkészülést, az észlelést és elemzést, az elszigetelést, a felszámolást és a helyreállítást." [7/2024. (VI. 24.) MK rendelet 2. melléklet 9.9. pont] (A, J, M: Kötelező)*

A fejezet kötelezővé teszi továbbá a biztonsági események nyomon követését és dokumentálását (9.25. pont), a személyzet jelentéstételi kötelezettségét és a jogszabály szerinti hatósági jelentést (9.27. pont), valamint a biztonsági eseménykezelési terv elkészítését, kihirdetését és karbantartását (9.34. pont); e követelmények mindhárom biztonsági osztályban (A, J, M) kötelezőek.

> *„9.27.1. Kötelezi a személyzetet arra, hogy jelentse a biztonsági esemény gyanúját vagy bekövetkeztét. 9.27.2. Jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat a jogszabályban meghatározott szervek felé." [7/2024. (VI. 24.) MK rendelet 2. melléklet 9.27. pont] (A, J, M: Kötelező)*

A biztonsági eseménykezelési terv tartalmi követelményei között a rendelet kifejezetten előírja a bejelentésköteles biztonsági események meghatározását, az eseménykezelés struktúrájának és felelőseinek rögzítését, valamint a terv rendszeres felülvizsgálatát [7/2024. (VI. 24.) MK rendelet 2. melléklet 9.34. pont]. Magasabb biztonsági osztályokban további követelmények lépnek be, így különösen az automatizált eseménykezelési és jelentési mechanizmusok (9.10., 9.28. pont), valamint az eseménykezelési képesség rendszeres tesztelése (9.5. pont), amelyek a „jelentős" és „magas" osztályban kötelezőek.

3.2.3 A hatósági bejelentési kötelezettség

Az eseménykezelési hatókör legmarkánsabb, az üzletmenet-folytonosságtól való elhatárolást leginkább megalapozó eleme a kötelező, határidőhöz kötött hatósági bejelentési rend, amelyet a Kiberbiztonsági tv. végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: Vhr.) 77–78. §-a rendez. A bejelentés címzettje az illetékes kiberbiztonsági incidenskezelő központ (a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete).

> *„1. indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 24 órán belül egy első bejelentést, amelyben – amennyiben az információk rendelkezésre állnak – fel kell tüntetni (...)" [418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 1. pont]*
> *„3. indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 72 órán belül egy eseménybejelentést, amely adott esetben aktualizálja az 1. pontban említett információkat, és tartalmazza az incidens első értékelését,*

beleértve annak súlyosságát és hatását;" [418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 3. pont]
„5. zárójelentést, legkésőbb a 3. pont szerinti eseménybejelentés benyújtását követő egy hónapon belül, amely tartalmazza a következőket: a) a kiberbiztonsági incidens részletes leírása, beleértve annak súlyosságát és hatását, b) a kiberbiztonsági incidenst valószínűleg kiváltó fenyegetés vagy kiváltó ok típusa, c) alkalmazott és folyamatban lévő mérséklési intézkedések, d) adott esetben a kiberbiztonsági incidens határokon átnyúló hatása;" [418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 5. pont]

Elhúzódó incidens esetén közbenső helyzetjelentés, a fertőzöttségi mutatók (IoC) tekintetében pedig azok rendelkezésre állásakor külön bejelentés szükséges, jelentős vagy nagykiterjedésű incidensnél a bejelentést rövid úton, telefonon is meg kell tenni [418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 2. pont, 78. § (2) bekezdés]. Hasonló, határidőhöz kötött külső jelentéstételi kötelezettséget az üzletmenet-folytonossági szabályozás nem tartalmaz: ez a bejelentési rezsim kizárólag az eseménykezelési hatókörhöz tartozik.

3.3 Az üzletmenet-folytonosság szabályozási hatóköre

Az üzletmenet-folytonosság követelményrendszerét az MK rendelet 2. mellékletének 7. fejezete (készenléti tervezés) tartalmazza. A fejezet hatóköre lényegesen tágabb, mint a kiberincidensek köre: minden olyan kiesési helyzetre kiterjed, amely az alapfeladatok és alapfunkciók működését veszélyezteti, ideértve az üzemzavart, a hardverhibát, az áramkimaradást, az emberi hibát és a természeti katasztrófát is, függetlenül attól, hogy az adott helyzet kiberbiztonsági incidensnek minősül-e.

A szervezetnek már „alap" biztonsági osztályban rendelkeznie kell üzletmenet-folytonossági szabályzattal és eljárásrenddel (7.1. pont), valamint az EIR-re vonatkozó üzletmenet-folytonossági tervvel (7.2. pont), amelynek kötelező tartalmi elemei a helyreállítási célok és prioritások.

„7.2.1. Kidolgozza az EIR-re vonatkozó üzletmenet-folytonossági tervet, amely: 7.2.1.1. meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket; 7.2.1.2. tartalmazza a helyreállítási célokat, a helyreállítási prioritásokat és metrikákat; (...)" [7/2024. (VI. 24.) MK rendelet 2. melléklet 7.2. pont] (A, J, M: Kötelező)

Szintén valamennyi biztonsági osztályban kötelező az elektronikus információs rendszer mentéseinek elkészítése és védelme, a helyreállítási idő- és helyreállítási pont célokkal (RTO, RPO) összhangban.

„7.35.1. Meghatározott gyakorisággal mentést készít az EIR-ben tárolt felhasználói szintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal. (...) 7.35.4. Megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre

> *állását mind az elsődleges, mind a biztonsági tárolási helyszínen." [7/2024. (VI. 24.) MK rendelet 2. melléklet 7.35. pont] (A, J, M: Kötelező)*

„Jelentős" és „magas" biztonsági osztályban a hatókör tovább bővül: kötelezővé válik az üzletmenet-folytonossági terv rendszeres tesztelése és a tesztelési eredmények alapján a terv javítása (7.13. pont), a biztonsági tárolási helyszín létrehozása és annak az elsődleges helyszíntől való megfelelő elkülönítése (7.19–7.20. pont), az alternatív feldolgozási helyszín kijelölése (7.23. pont), valamint a mentések megbízhatóságának és sértetlenségének tesztelése (7.36. pont).

> *„7.13.1. meghatározott gyakorisággal és meghatározott teszteken keresztül vizsgálja az EIR-re vonatkozó üzletmenet-folytonossági tervet a terv hatékonyságának és a szervezet felkészültségének felmérése céljából; (...)" [7/2024. (VI. 24.) MK rendelet 2. melléklet 7.13. pont] (J, M: Kötelező)*

Az üzletmenet-folytonossági követelmények teljesítése tehát alapvetően megelőző, tervezési, kapacitás- és tesztelési jellegű kötelezettségeket keletkeztet, amelyek folyamatosan, incidenstől függetlenül állnak fenn, és amelyek teljesülését elsősorban a kétévenkénti kiberbiztonsági audit, illetve a hatósági ellenőrzés vizsgálja.

3.4 A két terület eltérő hatókörének összevetése

A fentiek alapján a két szabályozási terület hatóköre az alábbi szempontok mentén határolható el egymástól:

- Kiváltó ok: az eseménykezelés hatókörét konkrét kiberbiztonsági esemény, incidensközeli helyzet vagy incidens (illetve annak gyanúja) nyitja meg; az üzletmenet-folytonosság hatóköre bármely, a rendelkezésre állást veszélyeztető kiesésre kiterjed, a kiváltó ok jellegétől függetlenül. Tehát az eseménykezelés jóval bővebb, mint az üzletmenet folytonosság területe.
- Cél: az eseménykezelés célja az incidens észlelése, elszigetelése, felszámolása, kivizsgálása és a jogszabályi bejelentések teljesítése, ugyanakkor egy incidens nem feltétlenül aktiválja az üzletmenet folytonossági terveket. Az üzletmenet-folytonosság célja az alapfeladatok előre meghatározott szintű működtetése és a helyreállítási célok (RTO, RPO) szerinti visszaállítás.
- Időhorizont: az eseménykezelés a tudomásszerzéstől a zárójelentésig terjedő, határidőkkel tagolt folyamat mely kiterjed az üzletmenet folytonosságot érintő eseteken túlra IS; az üzletmenet-folytonosság folyamatos, megelőző tevékenység, amely a tervezéstől a rendszeres tesztelésen át a tényleges kiesés kezeléséig tart.
- Kötelező dokumentumok: az eseménykezelés oldalán a biztonsági eseménykezelési szabályzat, eljárásrend és a biztonsági eseménykezelési terv (MK rendelet 2. melléklet 9.1. és 9.34. pont); az üzletmenet-folytonosság oldalán az üzletmenet-folytonossági szabályzat, eljárásrend és terv, valamint a mentési és helyreállítási dokumentáció (7.1., 7.2. és 7.35. pont).

- Hatósági kapcsolat: az eseménykezeléshez kötelező bejelentési rezsim tartozik (24 óra, 72 óra, zárójelentés), az üzletmenet-folytonossághoz önálló bejelentési kötelezettség nem kapcsolódik, teljesülését az audit és a hatósági ellenőrzés vizsgálja.
- Biztonsági osztálytól való függés: mindkét területen a szabályzat, a terv és az alapképesség már „alap” osztályban kötelező, a tesztelési, automatizálási és tartalék-helyszín követelmények jellemzően a „jelentős” és „magas” osztályban lépnek be.

3.5 A két terület kapcsolódási pontjai

Az eltérő hatókör ellenére a két terület a szabályozásban kifejezetten összekapcsolt. Az összekapcsolás első szintje maga az incidenskezelés törvényi fogalma, amely a működés helyreállítását is az incidenskezelés részévé teszi [2024. évi LXIX. törvény 4. § 47. pont]: egy jelentős incidens helyreállítási szakaszában a szervezet gyakorlatilag az üzletmenet-folytonossági tervét (mentések visszaállítása, alternatív helyszín aktiválása) hajtja végre. (Ugyanakkor mint említettük nem minden incidens aktiválja az üzletmenet folytonossági terveket)

A második szintet az MK rendelet kölcsönös összehangolási kötelezettségei adják. A rendelet mindkét fejezet oldaláról előírja a két terület tervezési tevékenységeinek egyeztetését.

> *„7.2.3. Összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;” [7/2024. (VI. 24.) MK rendelet 2. melléklet 7.2.3. pont] (A, J, M: Kötelező)*
> *„9.9.3. A szervezet összehangolja a biztonsági eseménykezelési tevékenységeket az üzletmenet-folytonossági tervezési tevékenységekkel.” [7/2024. (VI. 24.) MK rendelet 2. melléklet 9.9. pont] (A, J, M: Kötelező)*

Az összehangolás a tesztelésre is kiterjed: az üzletmenet-folytonossági terv tesztelését egyeztetni kell a kapcsolódó tervekért – köztük a biztonsági eseménykezelési tervért – felelős szervezeti egységekkel (7.14. pont), és fordítva, a biztonsági események kezelésének tesztelését is össze kell hangolni a kapcsolódó tervekkel (9.7. pont); mindkét követelmény a „jelentős” és „magas” osztályban kötelező.

A kapcsolódásnak van egy bejelentési vetülete is: a **jelentős** kiberbiztonsági incidens törvényi küszöbértékei (szolgáltatáskiesés, bevételkiesés, súlyos működési zavar) az üzletmenet-folytonossági tervezés során képzett üzleti hatásadatokból ítélhetők meg megalapozottan, a Vhr. szerinti első bejelentés kötelező tartalmi elemei között pedig szerepel a szolgáltatás helyreállításának várható időpontja is [418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 1. pont], amely érdemben csak az üzletmenet-folytonossági tervben rögzített helyreállítási célok ismeretében adható meg.

A gyakorlatban, a NIS2 auditra való felkészülés során ezért javasolt:

- a biztonsági eseménykezelési tervben rögzíteni azokat az eszkalációs kritériumokat, amelyek teljesülése esetén az incidenskezelés az üzletmenet-folytonossági terv (illetve a katasztrófa-helyreállítási terv) aktiválását vonja maga után;

- az üzletmenet-folytonossági tervben szereplő helyreállítási idő- és helyreállítási pont célokat (RTO, RPO) összhangba hozni az incidensbejelentésekben közlendő helyreállítási vállalásokkal;
- a két terület tesztjeit legalább részben közös forgatókönyvre (pl. zsarolóvírus-támadás miatti teljes helyreállítás) építeni, és a tesztek tanulságait mindkét tervbe visszavezetni;
- a felelősségi köröket úgy kijelölni, hogy az incidenskezelésért és az üzletmenet-folytonosságért felelős szerepkörök között a kapcsolattartás és a döntési jogosultság dokumentált legyen.

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 418/2024. (XII. 23.) Korm. rendelet a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2 irányelv)