

Be kell-e sorolni egy NIS2-kötelezett szervezet elektronikus információs rendszerei közé a kivezetés alatt álló, csak olvasható módban működő szoftvereket?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi
állásfoglalás 2026/39

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.23	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Igen. A kivezetés alatt álló, csak olvasható módban működő szoftver addig a szervezet elektronikus információs rendszere (EIR), amíg a szervezet rendelkezésében van és digitális adatokat tárol, keres vissza vagy jelenít meg. Az ilyen rendszert ugyanúgy nyilvántartásba kell venni és biztonsági osztályba kell sorolni, mint az aktívan használt rendszereket.

A Kiberbiztonsági tv. az EIR fogalmát a rendszer funkciója alapján határozza meg, és nem teszi függővé attól, hogy keletkezik-e még új adat a rendszerben. A törvény a teljes életciklusra, így a megszüntetés szakaszára is kockázatokkal arányos védelmet ír elő. A 7/2024. (VI. 24.) MK rendelet pedig kifejezetten a „meglévő rendszer kivezetését” említi olyan változásként, amelyet az EIR-nyilvántartásban át kell vezetni. A kivezetés alatt álló rendszerekre a jogszabályok nem tartalmazznak kivételt.

A csak olvasható üzemmód nem mentesít a besorolás alól, viszont olyan változás, amely miatt a kockázatelemzést és a biztonsági osztályba sorolást felül kell vizsgálni. A biztonsági osztály ilyenkor sem csökken automatikusan, mert azt elsősorban a megőrzött adatok bizalmassága határozza meg. A kivezetett szoftvereknél gyakori a gyártói támogatás megszűnése, ezt a védelmi intézkedések kiválasztásakor külön kezelni kell.

A rendszer akkor kerülhet ki a nyilvántartásból, ha a kivezetés ténylegesen lezárult: az adatokat átadták egy másik, szintén nyilvántartott rendszernek vagy biztonságosan törölték, a rendszerelemeket pedig leselejtezték. A lezárást dokumentálni kell, mert a kiberbiztonsági audit a szervezet valamennyi EIR-jének besorolását vizsgálja.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2¹-kötelezett szervezet (a továbbiakban: Szervezet) egyes szoftvereit kivezeti. Az átmeneti időszakban ezek a szoftverek csak olvasható módban működnek: új adat nem rögzíthető bennük, a korábban rögzített adatok azonban lekérdezhetők, például jogszabályi megőrzési kötelezettség, belső ellenőrzés vagy jogvita miatt. Be kell-e sorolni ezeket a szoftvereket a Szervezet elektronikus információs rendszerei közé, azaz fel kell-e venni őket az EIR-ek nyilvántartásába, és biztonsági osztályba kell-e sorolni őket? Ha igen, milyen hatása van a csak olvasható üzemmódnak a besorolásra, és mikor kerülhet ki a rendszer a nyilvántartásból?

A kivezetés alatt álló rendszerekre alkalmazandó védelmi intézkedések teljes körű meghatározása nem tárgya ennek az állásfoglalásnak.

¹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1792 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályaon kívül helyezéséről (NIS 2 irányelv)

3. VÁLASZ

3.1 A vizsgálat kiindulópontjai

Az állásfoglalás abból indul ki, hogy a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja alá tartozik, és kiberbiztonsági felügyeletét a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) látja el.² A válasz lényege a többi szervezettípusra is irányadó, az 1. § (1) bekezdés a)-c) és f) pontja alá tartozó szervezetek többsétkötelezettségeit a 3.6. pont foglalja össze.

A kérdés két kötelezettséget érint. Az egyik a Szervezet által használt EIR-ek felmérése és nyilvántartásba vétele³, a másik a rendelkezésében lévő EIR-ek biztonsági osztályba sorolása.⁴ Mindkettő arra a rendszerre vonatkozik, amely EIR-nek minősül, ezért a vizsgálatot a fogalomnál kell kezdeni.

3.2 A csak olvasható rendszer is EIR

3.2.1 A törvényi fogalom a funkcióhoz igazodik

A Kiberbiztonsági tv. az EIR fogalmát a rendszer által ellátott funkció alapján határozza meg:

24. elektronikus információs rendszer:

[...]

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy

c) az a) és b) alpontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok; [2024. évi LXIX. tv. 4. § 24. pont]

A fogalom egyik eleme sem kívánja meg, hogy a rendszerben új adat keletkezzen vagy meglévő adat módosuljon. A csak olvasható módban működő szoftver továbbra is program alapján, automatizáltan kezeli a digitális adatokat: tárolja, keresi, lekérdezi és megjeleníti őket. Ez a b) alpont feltételét teljesíti. A rendszerben megőrzött adatok a c) alpont szerint maguk is az EIR részei, hiszen tárolt és visszakeresett digitális adatokról van szó. Az adatkezelés fogalmát a Kiberbiztonsági tv. az Infotv.-ből veszi át⁵, amely a tárolást és a lekérdezést kifejezetten adatkezelési műveletként nevesíti.⁶ A magyar fogalom a NIS2 irányelv 6. cikk 1. pontjában meghatározott hálózati és információs rendszer fogalmát követi, amely szintén kiterjed a tárolt és visszakeresett digitális adatokra.

Az SZTFH a kiberbiztonsági auditról szóló tájékoztatójában ugyanezt a megközelítést követi: „Amennyiben a szervezet akár csak egy olyan eszközzel rendelkezik, amely egy szoftver segítségével képes digitális adatok feldolgozására, tárolására vagy továbbítására, az megalapozza

² 2024. évi LXIX. tv. 23. § (1) bekezdés b) pont

³ 2024. évi LXIX. tv. 6. § (3) bekezdés 1. pont; 7/2024. (VI. 24.) MK rendelet 2. melléklet 1.5. pont (A, J, M)

⁴ 2024. évi LXIX. tv. 6. § (3) bekezdés 5. pont és 10. § (1) bekezdés

⁵ 2024. évi LXIX. tv. 4. § 4. pont

⁶ 2011. évi CXII. tv. 3. § 10. pont

az elektronikus információs rendszer létét, így azt a 7/2024. (VI.24.) MK rendeletben foglaltak szerint biztonsági osztályba kell sorolni és az ennek megfelelő követelményeket teljesíteni szükséges.”⁷

3.2.2 A rendelkezési jog számít, nem a használat intenzitása

A törvény a szervezet EIR-jét a rendelkezési joghoz köti:

(1) A szervezet elektronikus információs rendszerének kell tekinteni a szervezet rendelkezésében lévő elektronikus információs rendszert. [2024. évi LXIX. tv. 6. § (1) bekezdés]

A biztonsági osztályba sorolás kötelezettsége is valamennyi, a szervezet rendelkezésében lévő EIR-re kiterjed:

(1) A szervezet elektronikus információs rendszerei, valamint az azokban kezelt adatok, a nyújtott szolgáltatások kockázatokkal arányos védelmének biztosítása érdekében a szervezet az e törvény hatálya alá tartozó, a szervezet rendelkezésében lévő elektronikus információs rendszereit „alap”, „jelentős” vagy „magas” biztonsági osztályba sorolja az érintett elektronikus információs rendszer sértetlensége és rendelkezésre állása, valamint az általa kezelt adat bizalmassága, sértetlensége és rendelkezésre állásának kockázata alapján, szigorodó védelmi előírásokkal. [2024. évi LXIX. tv. 10. § (1) bekezdés]

A kivezetés alatt álló szoftver felett a Szervezet továbbra is rendelkezik: ő dönt arról, ki férhet hozzá, meddig működik, és mi történik az adataival. Az, hogy a rendszert ritkán vagy már csak lekérdezésre használják, a rendelkezési jogon nem változtat. A törvény hatálya alól kivett rendszerek köre zárt. Ide a minősített adatot kezelő, a műveleti célú, az atomenergia alkalmazása körében meghatározott programozható rendszerek, valamint a kormányrendeletben kijelölt szerv kiberbiztonsági szolgáltatásai tartoznak.⁸ A kivezetés alatt álló vagy csak olvasható rendszerekre a törvény nem tartalmaz kivételt.

Ugyanez következik a kiberbiztonsági audit törvényi és eljárásrendi szabályaiból. A Kiberbiztonsági tv. 16. § (1) bekezdése alapján az auditor a szervezet információbiztonságának, a szervezet valamennyi elektronikus információs rendszere biztonsági osztályának, továbbá a védelmi intézkedések megfelelőségének átfogó vizsgálatát végzi el. A jogalkotó egyértelművé teszi, hogy az auditori vizsgálat hatóköre kiterjed a szervezet minden rendelkezésére álló, adatot kezelő elektronikus információs rendszerére, függetlenül attól, hogy az aktív vagy archív állapotban van.

Ha a nyilvántartásból hiányzik egy olyan rendszer, amely a Szervezet rendelkezésében van és adatot kezel, azt az auditor a vizsgálat során hiányosságként tárhatja fel. A hatósági gyakorlat is számol a kivezetett rendszerekkel: a nemzeti kiberbiztonsági hatóság besorolást támogató

⁷ Szabályozott Tevékenységek Felügyeleti Hatósága: A kiberbiztonsági audit rendje (tájékoztató), „Mi a teendő, amennyiben egy szervezet nem rendelkezik EIR-rel?” című rész, 16. oldal. Elérhető az SZTFH honlapján.

⁸ 2024. évi LXIX. tv. 3. § (1) bekezdés

úrlapján az EIR „használati státusza” „tervezett, üzemelő, archív vagy megszűnt” lehet⁹, vagyis az archív állapotú rendszer is a besorolás tárgya.

Ha a kivezetés alatt álló szoftvert a szállító üzemelteti, például felhőben tárolt archívumként, és a Szervezet rendelkezési joga csak a rendszer egyes elemeire vagy funkcióira terjed ki, a követelményeket ezekre az elemekre és funkciókra kell teljesíteni.¹⁰ A nyilvántartásba vétel és a besorolás kötelezettsége ilyenkor sem szűnik meg.

3.3 A kivezetés az életciklus része

A Kiberbiztonsági tv. az életciklus fogalmába a megszüntetést is beleérti:

26. életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam; [2024. évi LXIX. tv. 4. § 26. pont]

A védelmet pedig a teljes életciklusra előírja:

(1) Az e törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell
a) az elektronikus információs rendszerben kezelt adatok, információk és az elektronikus információs rendszerek által nyújtott vagy azon keresztül elérhető szolgáltatások bizalmassága, sértetlensége és rendelkezésre állása, valamint
b) az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása
vonatkozásában a zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet. [2024. évi LXIX. tv. 5. § (1) bekezdés]

A kivezetés tehát nem az életcikluson kívül eső állapot, hanem annak utolsó szakasza, amelyben a védelmi kötelezettség változatlanul fennáll. A 7/2024. (VI. 24.) MK rendelet ezt a kockázatmenedzsment keretrendszer szintjén is rögzíti:

1.1.7. a védelmi intézkedések folyamatos felügyeletével az elektronikus információs rendszer teljes életciklusa alatt gondoskodik arról, hogy a bekövetkezett szervezeti, technológiai és biztonsági környezetének változása esetén a védelmi intézkedések a kockázatokkal arányosak maradjanak. Ennek keretében
[...]

1.1.7.4. biztosítja, hogy a rendszer élesüzemből való kivonására vonatkozó terv tartalmazza a felmerülő kockázatok kezeléséhez tartozó intézkedéseket. [7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.7. pont]

⁹ Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet: Útmutató a 7/2024. MK rendelet szerinti biztonsági osztályba sorolást támogató űrlap 2.0 verziójához, 1.1 verzió, 4. oldal. Az űrlapot a nemzeti kiberbiztonsági hatóság felügyelete alá tartozó szervezetek használják.

¹⁰ 7/2024. (VI. 24.) MK rendelet 2. § (3) bekezdés

A csak olvasható üzemmódra való átállás jellemzően az élesüzemből való kivonás első lépése. A Szervezetnek ezért olyan kivezetési tervvel kell rendelkeznie, amely rögzíti az átmeneti időszak kockázatait és az azok kezelésére szolgáló intézkedéseket.

A nyilvántartásra vonatkozó követelmény kifejezetten említi a kivezetést:

1.5. A szervezet létrehozza és a szervezet EIR-jeiben bekövetkezett változások (pl.: új rendszer bevezetése, meglévő rendszer kivezetése) esetén frissíti, valamint a szervezet által meghatározott gyakorisággal felülvizsgálja az EIR-ek nyilvántartását. [7/2024. (VI. 24.) MK rendelet 2. melléklet 1.5. pont] (A, J, M)

A kivezetés tehát a nyilvántartás frissítésével jár, a rendszer azonban nem a kivezetés megkezdésekor kerül ki onnan. Álláspontunk szerint a csak olvasható üzemmódra való átállást a nyilvántartásban jelezni kell (például „kivezetés alatt” vagy „archív” állapottal), a rendszert pedig csak a kivezetés lezárásakor lehet onnan törölni vagy „megszűnt” állapotúként megjelölni (lásd a3.5. pontot).

3.4 A csak olvasható üzemmód hatása a biztonsági osztályra

3.4.1 A besorolást felül kell vizsgálni

A biztonsági osztályt a rendszerben kezelt adatok és a rendszer funkciói határozzák meg:

2.1.2. Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet a szervezet vezetője hagy jóvá, hatáselemzés alapján kell elvégezni. [...] [7/2024. (VI. 24.) MK rendelet 1. melléklet 2.1.2. pont]

Csak olvasható üzemmódban a rendszer funkciói szűkülnek, a kezelt adatok köre viszont jellemzően változatlan marad. A változás a besorolási szempontokat eltérően érinti. A sértetlenség és a rendelkezésre állás sérülésének hatása csökkenhet, mert a rendszer már nem támogat napi üzleti folyamatot, és nem keletkezik benne új adat. Ez nem érvényes, ha a megőrzött adatokhoz jogszabályi kötelezettség teljesítéséhez, meghatározott határidőn belül hozzá kell férni. A bizalmasság szempontjából a helyzet nem változik: ha a rendszer nagy mennyiségű személyes adatot vagy jogszabállyal védett titkot őriz, ezek sérülése a kivezetés alatt is közepes káreseményt okozhat, ami a „jelentős” osztály ismérve.¹¹ A biztonsági osztály tehát nem csökken automatikusan, azt a megőrzött adatok alapján kell újra megállapítani.

A kiberbiztonsági jogszabályok a biztonsági osztályba sorolás, a kockázatelemzés és az adatosztályozás során kívüli felülvizsgálatát az elektronikus információs rendszer kockázati környezetében bekövetkező jelentős változásokhoz kötik.¹² A d) pont szerinti szervezetekre a 7/2024. (VI. 24.) MK rendelet külön felülvizsgálati okot nem nevez meg, a kockázatelemzést azonban jelentős változás esetén frissíteni kell:

¹¹ 7/2024. (VI. 24.) MK rendelet 1. melléklet 2.2.3.1. és 2.2.3.3. pont

¹² 2024. évi LXIX. tv. 6. § és 8. §, valamint a 418/2024. (XII. 23.) Korm. rendelet 5. § (1) bekezdés

15.4. A szervezet:

[...]

15.4.6. Meghatározott gyakorisággal frissíti a kockázatelemzést vagy minden olyan esetben, amikor jelentős változások történnek a rendszerben, annak működési környezetében, vagy más olyan körülményekben, amelyek befolyásolhatják a rendszer biztonsági állapotát. [7/2024. (VI. 24.) MK rendelet 2. melléklet 15.4. pont] (A, J, M)

Mivel a biztonsági osztály a kockázatelemzésre épül, a csak olvasható üzemmódra való átálláskor a besorolás dokumentált felülvizsgálata indokolt. Az üzemmód megváltoztatása előtt vizsgálni kell annak információbiztonsági hatásait¹³, az eredményt pedig a rendszerbiztonsági tervben át kell vezetni.¹⁴

3.4.2 A vezető döntése a használat folytatásáról

A biztonsági osztályba sorolásról a szervezet vezetője dönt¹⁵, és ő dönt az EIR-ek használatának folytatásáról is.¹⁶ Álláspontunk szerint a csak olvasható üzemmódra való átállás olyan változás, amely után a vezetőnek a 7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.6. pontja szerint, jegyzőkönyvben dokumentált módon kell döntenie a rendszer használatának folytatásáról. A döntést a felülvizsgált kockázatelemzésre, a frissített rendszerbiztonsági tervre és a kivezetési tervre kell alapozni, és célszerű benne rögzíteni a kivezetés tervezett befejezésének időpontját is.

3.4.3 Eltérés a védelmi intézkedésektől

A csak olvasható üzemmód nem mentesít a biztonsági osztályhoz tartozó követelmények alól, de indokolhat dokumentált eltérést:

3.2.4.2. A védelmi intézkedések az elektronikus információs rendszer csak azon komponenseire vonatkoznak, amelyek az intézkedés által megcélzott biztonsági képességet biztosítják vagy támogatják, és az intézkedés által csökkenteni kívánt lehetséges kockázatok forrásai. [7/2024. (VI. 24.) MK rendelet 1. melléklet 3.2.4.2. pont]

Ha a rögzítési, módosítási vagy adatcsere-funkciókat ténylegesen megszüntették, az ezekhez kötődő egyes intézkedések alkalmazása okafogyottá válhat. Az eltérést a Szervezet szabályozásában dokumentálni és indokolni kell, a dokumentumot pedig a vezető vagy a kockázatok felvállalására jogosult személy hagyja jóvá.¹⁷ A Kiberbiztonsági tv. 2. és 3. melléklete szerinti szervezetnek minősülő szervezetek a védelmi intézkedések fokozatos bevezetésére vonatkozó eltérést nem alkalmazhatják¹⁸, így a kivezetés alatt álló rendszer arra hivatkozva sem hagyható védelem nélkül, hogy hamarosan megszűnik.

¹³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.15. pont (A, J, M)

¹⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.2. pont (A, J, M)

¹⁵ 2024. évi LXIX. tv. 10. § (2) bekezdés

¹⁶ 2024. évi LXIX. tv. 6. § (3) bekezdés 12. pont

¹⁷ 7/2024. (VI. 24.) MK rendelet 1. melléklet 3.1.2. és 3.1.3. pont

¹⁸ 7/2024. (VI. 24.) MK rendelet 3. §

3.5 A kivezetés alatt álló rendszerek jellemző kockázatai

A kivezetett szoftverek egy részét a gyártó már nem támogatja, biztonsági frissítés nem érkezik hozzájuk. Erre a helyzetre önálló követelmény vonatkozik:

16.99. A szervezet:

16.99.1. lecseréli a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól; illetve

16.99.2. a támogatással már nem rendelkező rendszerelemekhez alternatív támogatást biztosít, amelyet belső erőforrásokkal vagy a szervezet által meghatározott külső szolgáltatók bevonásával valósít meg.

[7/2024. (VI. 24.) MK rendelet 2. melléklet 16.99. pont] (A, J, M)

Maga a kivezetés is a 16.99.1. pont szerinti csere egyik módja lehet, ha belátható időn belül lezárul. Az átmeneti időszakra azonban a Szervezetnek dokumentálnia kell, hogyan kezeli a támogatás hiányát. A hibajavításra vonatkozó követelmény¹⁹ a kivezetés alatt is alkalmazandó. Ha javítás már nem érhető el, helyettesítő védelmi intézkedésre van szükség, ilyen lehet a rendszer hálózati elkülönítése, a hozzáférés szűk körre korlátozása vagy a szükségtelen interfészek lekapcsolása. A helyettesítő intézkedés feltételeit, köztük a kockázat felmérését, elfogadását és a vezetői jóváhagyást a 7/2024. (VI. 24.) MK rendelet 1. melléklet 4.2. pontja határozza meg.

A csak olvasható üzemmód maga is védelmi intézkedésként kezelhető. A rendszert úgy kell konfigurálni, hogy csak az üzletmenet szempontjából szükséges szolgáltatásokat nyújtsa²⁰, a fiókkezelést pedig a megváltozott használatához kell igazítani.²¹ Jelentős és magas osztályú rendszernél a hozzáférést a legkisebb jogosultság elve szerint azokra kell korlátozni, akiknek a lekérdezésre ténylegesen szükségük van²², és a rendszert a sérülékenységmentes menedzsmentből sem lehet kihagyni.²³

3.6 Mikor kerülhet ki a rendszer a nyilvántartásból?

A rendszer addig marad a nyilvántartásban, amíg a Szervezet rendelkezésében van és adatot kezel. A kivezetés lezárásához három kérdést kell rendezni.

Az első az adatok sorsa. A Szervezetnek a rendszerben lévő és onnan kikerülő információkat a jogszabályi és működési követelmények szerint kell kezelnie és megőriznie:

18.67. A szervezet az EIR-ben lévő és az onnan kikerülő információk kezelése és megőrzése során a szervezetre vonatkozó, hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások és működési követelmények szerint jár el. [7/2024. (VI. 24.) MK rendelet 2. melléklet 18.67. pont] (A, J, M)

¹⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 18.2. pont (A, J, M)

²⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.26. pont (A, J, M)

²¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 2.2. pont (A, J, M)

²² 7/2024. (VI. 24.) MK rendelet 2. melléklet 2.60. pont (J, M)

²³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 15.10. pont (J, M)

Ha a megőrzési kötelezettség a kivezetés után is fennáll (ilyen például a számviteli bizonylatok nyolcéves megőrzése²⁴), az adatokat egy másik rendszerbe, például archívumba vagy az utódrendszerbe kell átvinni. Az adatok ezzel nem kerülnek ki a Kiberbiztonsági tv. hatálya alól. A befogadó rendszer maga is EIR, az átvett adatok pedig a fogalom c) alpontja szerint annak részévé válnak, ezért a befogadó rendszer besorolásánál ezeket is figyelembe kell venni. A kivezetett rendszer biztonsági igénye tehát nem szűnik meg, hanem átkerül a befogadó rendszerhez.

A második a rendszerelemek sorsa. A leselejtezésre kerülő adathordozókat biztonságos törlési technikákkal kell törölni²⁵, a rendszerelemeket meghatározott módszerekkel kell selejtezni²⁶, jelentős vagy magas osztályú rendszernél pedig a rendszerelem-leltárt az eltávolításkor frissíteni kell.²⁷

A harmadik a dokumentáció. A kivezetés lezárását az EIR-ek nyilvántartásában át kell vezetni.²⁸ Célszerű a rendszert nem egyszerűen törölni, hanem „megszűnt” állapotúként, a megszűnés időpontjával és a lezárást igazoló dokumentumokra (adatmigrációs, törlési és selejtezési jegyzőkönyv) való hivatkozással megtartani a nyilvántartásban. A kiberbiztonsági auditot kétfévente kell elvégeztetni²⁹, és a két audit között kivezetett rendszereknél ezek a dokumentumok igazolják, hogy a rendszer jogszerűen került ki a nyilvántartásból.

3.7 A közsférába tartozó szervezetek többletkötelezettségei

Ha a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) vagy f) pontja alá tartozik, a 418/2024. (XII. 23.) Korm. rendelet szervezeti kötelezettségekre vonatkozó rendelkezései is alkalmazandók.³⁰ Ezeknél a szervezeteknél a biztonsági osztályba sorolás soron kívüli felülvizsgálatára kifejezett szabály vonatkozik:

- (1) A szervezet soron kívül felülvizsgálja a biztonsági osztályba sorolást, ha az elektronikus információs rendszer kockázati környezetében vagy az adatosztályozásban változás következik be.*
- (2) A biztonsági osztályba sorolás felülvizsgálatának eredményét a szervezet 15 napon belül megküldi a nemzeti kiberbiztonsági hatóság részére. [418/2024. (XII. 23.) Korm. rendelet 5. § (1) és (2) bekezdés]*

Álláspontunk szerint a csak olvasható üzemmódra való átállás a kockázati környezet változásának minősül, ezért a felülvizsgálat eredményét 15 napon belül meg kell küldeni a hatóságnak. A hatóság besorolást támogató űrlapja erre az „archív” állapot megjelölésével lehetőséget ad. Az adatosztályozásra kötelezett szervezeteknek a biztonsági osztályba sorolás keretében az adatosztályozást is felül kell vizsgálniuk.³¹

²⁴ 2000. évi C. tv. 169. § (2) bekezdés

²⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 11.8. pont (A, J, M)

²⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.27. pont (A, J, M)

²⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.37. pont (J, M)

²⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 1.5. pont (A, J, M)

²⁹ 2024. évi LXIX. tv. 16. § (1) bekezdés

³⁰ 418/2024. (XII. 23.) Korm. rendelet 1. § (1) bekezdés

³¹ 2024. évi LXIX. tv. 9. § (5) bekezdés

3.8 A javasolt eljárás

A kivezetést célszerű az alábbi lépésekben végrehajtani:

- a) Felmérés, a kivezetés alatt álló, csak olvasható módban működő szoftverek azonosítása, nyilvántartásba vételük vagy nyilvántartási adataik frissítése „kivezetés alatt” állapottal és a kivezetés tervezett befejezésének időpontjával.
- b) Felülvizsgálat, a kockázatelemzés és a biztonsági osztályba sorolás felülvizsgálata a megőrzött adatok alapján, a rendszerbiztonsági terv frissítése, a vezető jegyzőkönyvezett döntése a használat folytatásáról.
- c) Kivezetési terv, az átmeneti időszak kockázatainak és kezelésüknek, az adatok megőrzési idejének, a migráció módjának és a felelősöknek a rögzítése.
- d) Átmeneti védelem, a csak olvasható működés technikai kikényszerítése, a hozzáférések szűkítése, a támogatás hiányának kezelése helyettesítő intézkedésekkel, az indokolt eltérések dokumentálása és jóváhagyása.
- e) Lezárás, az adatok átadása a befogadó rendszernek vagy biztonságos törlésük, a rendszerelemek selejtezése, a leltár és az EIR-nyilvántartás frissítése, a lezárást igazoló dokumentumok megőrzése a kiberbiztonsági audithoz.
- f) Hatósági bejelentés az a)-c) és f) pont szerinti szervezeteknél a felülvizsgált besorolás megküldése a nemzeti kiberbiztonsági hatóságnak 15 napon belül.

4. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS 2 irányelv)
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)
- 2000. évi C. törvény a számvitelről
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- NBSZ Nemzeti Kiberbiztonsági Intézet: Útmutató a 7/2024. MK rendelet szerinti biztonsági osztályba sorolást támogató űrlap 2.0 verziójához (1.1 verzió)