Hogyan ellenőrizheti egy NIS2 kötelezett cég az általa megbízott közreműködő kiberbiztonsági megfelelését?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/18

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.20	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A kiberbiztonsági törvény és a 7/2024. MK rendelet előírja, hogy a közreműködőkkel kapcsolatos kockázatokat az ellátási lánc részeként azonosítani, dokumentálni és folyamatosan kezelni kell, ideértve a kockázatokkal arányos követelmények szerződésbe foglalását, a konkrét védelmi intézkedések kikényszerítését, valamint a rendszeres beszállítói értékelést is.

A vezetés közvetlen feladata, hogy a fejlesztésre, üzemeltetésre, karbantartásra, felhőszolgáltatásra vagy incidenskezelésre szerződő partnerekkel szemben világos biztonsági osztályt és felelősségmegosztást rögzítsen, és ennek teljesülését belső és külső ellenőrzésekkel is vizsgálja.

A jogszabályi minimumon túl további, szerződésben kiköthető eszközök, jelentősen csökkenthetik a kritikus rendszerekre gyakorolt beszállítói kockázatot. Ilyen például a megrendelő által audit lehetősége, információbiztonsági tanúsítványok (pl. ISO 27001), NIS2 audit elvárása, rendszeres sérülékenységvizsgálat és penetrációs teszt, szigorúbb SLA-k, forráskód-letét (escrow).

2. A VIZSGÁLANDÓ KÉRDÉS

Adott egy NIS2 kötelezett cég, aki szerződik egy közreműködővel (pl szoftverszállító)

A vele szerződő közreműködővel szemben milyen ellenőrzési kötelezettségei vannak?

A vele szerződő közreműködővel szemben milyen ellenőrzési lehetőségei vannak a kötelező ellenőrzéseken túl?

3. VÁLASZ

3.1 A közreműködővel szembeni kötelező ellenőrzési kötelezettségek

A NIS2 irányelvet átültető 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) és a végrehajtására kiadott 7/2024. (VI. 24.) MK rendelet (a továbbiakban: MK rendelet) a "bizalom a láncolatban" elvét követi. Ez azt jelenti, hogy az érintett szervezet nem háríthatja át a felelősséget a közreműködőre (pl. szoftverszállítóra), hanem köteles gondoskodni arról, hogy a szállító is megfeleljen a biztonsági követelményeknek.

A jogszabályok alapján a következő konkrét kötelezettségek terhelik a NIS2 kötelezett céget a közreműködővel szemben:

- Kockázatokkal arányos követelmények szerződésbe foglalása
- Ellátási lánc kockázatainak kezelése
- Konkrét védelmi intézkedések kikényszerítése

- Ellátási lánc ellenőrzések

A szervezet vezetőjének közvetlen felelőssége, hogy ha közreműködőt vesz igénybe (legyen szó fejlesztésről, üzemeltetésről vagy karbantartásról), akkor a biztonsági követelményeket szerződéses úton kikényszerítse. Ez nem csupán lehetőség, hanem törvényi kötelezettség.

> *Ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, felhőszolgáltatás, illetve a kiberbiztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási tevékenységének a megvalósításához, gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben a kockázatokkal arányos szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek; [2024. évi LXIX. törvény 6. § (5) bekezdés d) pont]*

Az MK rendelet 1. melléklete (kockázatmenedzsment keretrendszer) előírja, hogy a szervezetnek azonosítania kell a rendszerrel kapcsolatos fenyegetettségeket, beleértve a beszállítói láncot is. A szervezetnek dokumentálnia kell a rendszer tervezésében, fejlesztésében és üzemeltetésében érintett szervezeteket.

> *1.1.1.2. az elektronikus információs rendszerekre vonatkozóan meghatározza és dokumentumban rögzíti*
> *[...] 1.1.1.2.2. a tervezésben, fejlesztésben, implementálásban, üzemeltetésben, karbantartásban, használatban és ellenőrzésben érintett személyeket vagy szervezeteket,*
> *[7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.1.2.2. pont]*

Az MK rendelet 2. melléklete (Védelmi intézkedések katalógusa) konkrét kontrollokat ír elő, amelyeket a szervezetnek érvényesítenie kell a közreműködővel szemben. Ezek a követelmények a biztonsági osztálytól (Alap, Jelentős, Magas) függően kötelezőek.

A beszerzések során a szerződésben rögzíteni kell a funkcionális biztonsági követelményeket és a felelősségmegosztást.

> *16.7. A szervezet a beszerzési folyamat során – beleértve a fejlesztést, az adaptálást, a rendszerkövetést és a karbantartást is – a szerződéseiben egységes nyelvezetet alkalmaz, továbbá követelményként rögzíti az alábbiakat:*
> *[...] 16.7.4. Az érintett EIR biztonsági osztályát és az ahhoz tartozó, illetve a szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedéseket.*
> *[...] 16.7.8. A felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását.*

[7/2024. (VI. 24.) MK rendelet 2. melléklet 16.7. pont] (A, J, M: Kötelező)

Külső rendszerek és szolgáltatások igénybevételekor a szervezetnek ellenőriznie kell a szolgáltató megfelelését.

16.49. A szervezet:
16.49.1. Szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett EIR-ek szolgáltatásai megfeleljenek a szervezet elektronikus információbiztonsági követelményeinek, és a szervezet által meghatározott védelmi intézkedéseket alkalmazzák.
[...] 16.49.3. külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső EIR szolgáltatója megfelel-e az elvárt védelmi intézkedéseknek.
[7/2024. (VI. 24.) MK rendelet 2. melléklet 16.49. pont] (A, J, M: Kötelező)

A közreműködőnek nemcsak a saját tevékenységére, hanem az általa igénybe vett alvállalkozókra is érvényesítenie kell a biztonsági követelményeket ("továbbadási kötelezettség").

19.7. A szervezet gondoskodik arról, hogy az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződései is tartalmazzák.
[7/2024. (VI. 24.) MK rendelet 2. melléklet 19.7. pont] (A, J, M: Kötelező)

Továbbá a szervezet köteles a beszállítókat és az általuk jelentett kockázatokat rendszeresen értékelni.

19.16. A szervezet meghatározott gyakorisággal értékeli és felülvizsgálja a beszállítókkal vagy szerződéses partnerekkel, illetve az általuk biztosított EIR-rel, rendszerelemmel vagy rendszerszolgáltatással kapcsolatos ellátási láncból eredő kockázatokat.
[7/2024. (VI. 24.) MK rendelet 2. melléklet 19.16. pont] (J, M: Kötelező; A: Opcionális [-])

3.2 A közreműködővel szembeni további (nem kötelező, de lehetséges) ellenőrzési lehetőségek

A jogszabályi minimumkövetelményeken túl a NIS2 kötelezett cég számos egyéb eszközzel csökkentheti a kockázatokat. Ezek alkalmazása különösen ajánlott, ha a közreműködő kritikus rendszerekhez fér hozzá, vagy ha a szervezet "Jelentős" vagy "Magas" biztonsági osztályba tartozik.

Az alábbi lehetőségek szerződéses szabadság keretében köthetők ki:

- Auditálási jog kikötése esetén a szervezet fenntarthatja magának a jogot a szerződésben, hogy ő maga, vagy az általa megbízott független auditor a helyszínen vagy távolról ellenőrizze a szoftverszállító biztonsági folyamatait. Ez túlmutat a puszta nyilatkozatok elfogadásán. Megjegyzés: Bár a jogszabály a 16.49.3. pontban előírja az ellenőrzést, annak mélysége és módja (pl. helyszíni audit) a felek megállapodásán múlhat, különösen alacsonyabb kockázat esetén.A szervezet előírhatja, hogy a közreműködő rendelkezzen elismert nemzetközi információbiztonsági tanúsítványokkal. Bár a törvény bizonyos esetekben előírhat tanúsított termékek használatát, a szervezet saját hatáskörben is szigoríthat. Ilyen tanúsítványok lehetnek például: ISO/IEC 27001 (Információbiztonsági irányítási rendszer), ISAE 3402 / SOC 2
- Rendszeres sérülékenységvizsgálat és behatolástesztelés (Penetration Testing) előírásával különösen szoftver fejlesztés esetén a megrendelő kikötheti, hogy a szállító köteles rendszeresen (pl. évente vagy minden főverzió kiadása előtt) független féllel behatolástesztet végeztetni, és a javítási jegyzőkönyvet átadni.

- Szigorúbb SLA (Service Level Agreement) és rendelkezésre állási garanciák alkalmazásával a jogszabályi "kockázatokkal arányos" védelemnél szigorúbb rendelkezésre állási és hibaelhárítási időket lehet meghatározni, kötbér terhe mellett.
- Forráskód letétbe helyezésével (Escrow), egyedi szoftverfejlesztésnél, az üzletmenet-folytonosság biztosítása érdekében (ha a szállító jogutód nélkül megszűnne), a szervezet kérheti a forráskód letétbe helyezését egy független harmadik félnél.
- Ellátási lánc átláthatósága (Software Bill of Materials – SBOM) előírásával a szervezet kérheti a szoftverszállítótól, hogy biztosítson részletes listát a szoftverben használt összes komponensről (beleértve a nyílt forráskódú könyvtárakat is), ami segíti a sebezhetőségek gyorsabb azonosítását. Az alábbi követelmény teljesítéséhez az SBOM kérése egy kiváló, bár nem expliciten kötelező eszköz

> *15.5. A szervezet:*
> *15.5.1. Felméri az ellátási lánc kockázatait a meghatározott EIR-ei, rendszerelemei és rendszerszolgáltatásai vonatkozásában.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 15.5. pont] (A, J, M: Kötelező)*

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról