Mit tehet egy NIS2 kötelezett cég, ha egy szerződött közreműködő megtagadja az együttműködést?

VFP2 KiberVéd - NIS2 Audit felkészítés
jogi állásfoglalás 2026/28

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.27	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A jelen állásfoglalás azt vizsgálja, milyen mozgástere van egy NIS2 hatálya alá tartozó szervezetnek, ha egy szerződött partnere közreműködője (például egy szoftverszállító) megtagadja a kiberbiztonsági együttműködést.

A kiberbiztonsági felelősséget a kötelezett cég nem háríthatja át partnereire; a megfelelés hiányáért a szervezet vezetője a felelős. A közreműködőknek szerződésben kell vállalniuk a biztonsági követelmények teljesítését.

Ha a közreműködő nem hajlandó együttműködni, a szervezet információbiztonsági felelőse (IBF) törvényi felhatalmazás alapján hivatalos adatkérést indíthat. A cég érvényesítheti auditálási jogát, illetve szerződéses szankciókat (pl. kötbér, díjcsökkentés) alkalmazhat, súlyos esetben pedig felmondhatja a szerződést. A fennmaradó ellátási lánc kockázatokat fizikai, logikai és adminisztratív kontrollokkal, vagy alternatív beszállítók bevonásával kell csökkenteni.

Az SZTFH főszabály szerint nem bírságolhatja közvetlenül a közreműködőt a mulasztásáért. A hatóság csak akkor járhat el közvetlenül a partnerrel szemben, ha az saját jogán is a Kiberbiztonsági tv. hatálya alá esik (például kihelyezett szolgáltató). Minden egyéb esetben a hatósági jogkövetkezmények a megrendelőt sújtják, akinek magánjogi eszközökkel (szerződésszegés megállapítása, kártérítés) kell fellépnie a partnerrel szemben.

2. A VIZSGÁLANDÓ KÉRDÉS

Adott egy NIS2 kötelezett cég, amelynek van egy szerződött partnere, amely a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) szerint közreműködőnek minősül. Kérdések:

Mit tehet az adott cég, ha a partner nem működik együtt a kiberbiztonsági követelmények teljesítésében?

A hatóság szabhat-e ki szankciókat a közreműködővel szemben, ha nem teljesíti a Kiberbiztonsági törvényben vagy a 7/2024 (VI.24) MK rendeletben foglalt kötelezettségeit?

3. VÁLASZ

3.1 Mit tehet az adott cég ha a partner nem működik együtt a kiberbiztonsági követelmények teljesítésében?

A Kiberbiztonsági törvény egyértelművé teszi, hogy az érintett szervezet nem háríthatja át a kiberbiztonsági felelősséget a közreműködő partnereire.

A jogszabály előírja, hogy a közreműködőknek is meg kell felelniük a biztonsági követelményeknek, és ezt a kötelezett cégnek szerződéses úton kell kikényszerítenie.

A jogszabály azt is rögzíti, hogy a megfelelés hiányáért a kötelezett cég vezetője a felelős az alábbiak szerint:

> *az (5) bekezdésben meghatározott feladatokért a szervezet vezetője az (5) bekezdés d) pontjában meghatározott esetben is felelős, kivéve az igénybe*

> *vett szolgáltatások mértékéig azokat az esetköröket, amikor központi szolgáltatót vagy központi rendszert kell a szervezetnek igénybe vennie. [2024. évi LXIX. tv. 4. § (6) bekezdés]*

A közreműködőnek szerződésben kell vállalnia azokat a kiberbiztonsági követelményeket, amelyek lehetővé teszik a NIS2 kötelezett szervezet számára a Kiberbiztonsági tv. és a 7/2024. (VI. 24.) MK rendelet (MK rendelet) előírásainak betartását, különös tekintettel az ellátási láncra vonatkozó előírásokra.

> *ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, a kiberbiztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási feladatok ellátásához, gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben a szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek; [2024. évi LXIX. tv. 4. § (5) bekezdés d) pont]"*

Az elvárt együttműködés területei (amelyek szerződéses kötelemként megjelenhetnek):

1. Információbiztonsági és audit kritériumok teljesítése, a feleknek együtt kell működniük a NIS2 audit sikeressége érdekében, különösen az információbiztonsági és audit kritériumok teljesítésére kiterjedően.

2. Incidenskezelés és tájékoztatás, a szolgáltató köteles monitorozni az információbiztonsági rendszereit, megvizsgálni a log adatokat és gondoskodni azok biztonságos tárolásáról. Továbbá köteles az általa észlelt minden információbiztonsági eseményről haladéktalanul (de legkésőbb X órán belül) átadni a rendelkezésre álló információt a megrendelőnek (az érintett NIS2 kötelezett cégnek), hogy az be tudja jelenteni az illetékes hatóságok felé.

3. Vizsgálatban való kooperáció, a közreműködő köteles átadni például egy incidensben érintett napló állományokat a megrendelőnek további vizsgálat céljából, és együttműködni a vizsgálat lefolytatása során.

4. Szerződésmódosítás, jogszabály-módosítás esetén a feleknek egyeztetniük kell, és szükség esetén a fennálló szerződésüket közösen módosítaniuk kell.

5. Egyéb a 7/2024 (VI.24) MK rendelet által előírt kötelezettségek.

A cég által kijelölt elektronikus információs rendszer biztonságáért felelős személy (IBF) erős törvényi felhatalmazással rendelkezik a partnerek ellenőrzésére. Ha a partner nem működik együtt, az IBF közvetlenül is felléphet és adatokat követelhet:

> *Az elektronikus információs rendszer biztonságáért felelős személy jogosult a szervezet elektronikus információbiztonsági kötelezettségeinek teljesítésében közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében jogosult megismerni a követelményeknek való megfelelőség alátámasztásához szükséges közre-*

működői tevékenységgel kapcsolatos adatot, valamint az érintett elektronikus információs rendszerek biztonsága tárgyában keletkezett valamenynyi dokumentumot. [2024. évi LXIX. tv. 7. § (6) bekezdés]

Amennyiben a beszállító (közreműködő) elzárkózik a kooperáció alól, és ezzel megsérti a szerződésben vállalt kötelezettségeit, az érintett NIS2 kötelezett szervezet (Megrendelő) a következő lépéseket teheti:

- Hivatalos adatkérés indítása az információbiztonsági felelősön keresztül, amelynek megtagadása esetén a partner egyértelműen jogszabályba és szerződésbe ütközően jár el.
- Szerződéses szankciók alkalmazása. Ha a felek a szerződésben rögzítették az együttműködési kötelezettséget, annak elmulasztása súlyos szerződésszegésnek minősül, amely megalapozza a szerződés felmondását. A NIS2-kompatibilis szerződéseknek tartalmazniuk kell, hogy a biztonsági követelmények nem teljesítése milyen következményekkel jár, mint például kötbér, díjcsökkentés, a szolgáltatás felfüggesztése vagy a szerződés felmondása.
- Auditálási jog gyakorlása, a szervezetnek kritikusan fontos ellenőriznie, hogy rendelkezik-e auditálási joggal a szerződésben, amely lehetővé teszi a beszállító tevékenységének ellenőrzését (pl. dokumentumellenőrzés, helyszíni audit, szabálytalanságok feltárása utáni intézkedési kötelezettség).
- Kockázatkezelés és alternatívák biztosítása, az érintett szervezetnek folyamatosan monitoroznia és értékelnie kell a rendszereit és a védelmi intézkedéseket, beleértve a beszállítói kapcsolatokat is. Ha a beszállító nem működik együtt, az növeli az ellátási lánc kockázatát. A szervezetnek figyelembe kell vennie a szolgáltatás megszűnéséből eredő kockázatokat, és redundanciákat vagy alternatívákat kell biztosítania a folytonosság fenntartására.

Alapvetően ha egy szállító nem jelez vissza a kockázatértékelésre, nem hajlandó adatot adni az információbiztonsági kontrolljai, alkalmazott gyakorlata kapcsán, akkor a megrendelőnek úgy kell minősítenie a szállítót, mint aki nem felel meg az elvárt biztonsági követelményeknek. Ez egy olyan, a jogviszony tartalmától /minőségétől/ a szállító leválthatóságától is függő kockázat lesz, amit a klasszikus:

- logikai
- fizikai
- adminisztratív (tipikusan jogi)
- intézkedésekkel tud csökkenteni, vagy ha nem képes a kockázatokat elfogadható szintre csökkenteni, a szerződést meg kell szüntetnie a szállítóval (amennyiben van alternatív szállító bevonására lehetősége).

Példa:

Egy szoftver fejlesztésbe bevont szervezet által használt fejlesztői eszközök biztonsági szintje nem meghatározható mert nem szolgáltat információt ehhez a megrendelőnek. Ebben az esetben azt kell feltételezni, hogy az eszközök nem felelnek meg semmilyen elvárásnak, kockázatot jelentenek. Megrendelő az alábbi kockázatcsökkentő eszközöket használhatja:

- megkövetelheti, hogy a fejlesztés során saját környezetében végezzenek munkát pl. távoli asztalon keresztül, korlátozva a ki-bemeneti adatok körét, legalább 2 faktoros autentikációt követelve meg a biztosított környezet eléréséhez,
- a szerződéssel okozott károk között kiemeli a megállapodásban az együtt nem működés eredményeként fennálló kockázatokból eredő károkat, és a kárfelősséget áttelepíti a szállítóra, esetleg megköveteli szakmai felelősségbiztosítás kötését / óvadék letétbe helyezését/ kötbér megfizetését ilyen esetekre,
- az átadott eredményeterméket maga vonja sérülékenységvizsgálat/ code review alá stb, esetleg 3 felet von be az eredménytermékek biztonsági szempontú értékelésének elvégzésébe.

3.2 A hatóság szabhat-e ki szankciókat a közreműködővel szemben, ha nem teljesíti a Kiberbiztonsági törvényben vagy a 7/2024(VI.24) MK rendeletben foglalt kötelezettségeit?

A hatályos jogszabályok értelmében az Szabályozott Tevékenységek Felügyeleti Hatóság főszabály szerint nem szabhat ki közvetlenül hatósági szankciót (például bírságot) a közreműködővel szemben, a közreműködő mulasztása esetén.

A hatóság kizárólag abban az esetben járhat el közvetlenül a partnerrel szemben, és szabhat ki rá szankciót, ha a szóban forgó közreműködő a saját tevékenysége jogán maga is közvetlenül a Kiberbiztonsági tv. hatálya alá esik. Ilyenek lehetnek például az alábbi, önálló törvényi kötelezettnek minősülő szolgáltatók:

- a felhőszolgáltatók, amelyek szolgáltatásuk okán az ágazati besorolás hatálya alá esnek,
- a kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltatók,
- a kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltatók.

Ilyen esetekben a hatóság a partnert nem mint egy másik cég "közreműködőjét", hanem mint önálló alapvető vagy fontos szervezetet vonja felelősségre a saját biztonsági hiányosságai okán.

Mivel a 7/2024. (VI. 24.) MK rendelet, valamint a Kiberbiztonsági tv. követelményeinek be nem tartása esetén a hatósági jogkövetkezmények (például információbiztonsági felügyelő kirendelése vagy bírság) a kötelezett szervezetet sújtják, a kötelezettnek magánjogi eszközöket kell alkalmaznia az együtt nem működő közreműködővel szemben. A szervezet a következő lépéseket teheti meg:

- szerződésszegés megállapítása, amely a jogszabályi megfelelés akadályozása miatt kártérítési felelősséget vonhat maga után,
- a szerződésben előzetesen kikötött kötbér, vagy egyéb szankciók és levonások érvényesítése,
- a partneri szerződés azonnali hatályú felmondása, amennyiben a közreműködő a biztonsági osztályhoz tartozó követelmények érvényesülését súlyosan veszélyezteti.

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény 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