

Egy külső fejlesztő által üzemeltett szoftver a fejlesztő vagy a megrendelő EIR-je?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi
állásfoglalás 2026/15

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.25	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Azt a kérdést, hogy egy külső fejlesztő által üzemeltett szoftvert a fejlesztő vagy a megrendelő elektronikus információs rendszerének (EIR) kell-e tekinteni, a konkrét szoftver, a szerződés és a vonatkozó dokumentáció ismeretében lehetséges megválaszolni. Olyan szoftvert, amelyet a fejlesztőcéggel termékként elad a megrendelő számára, de a megrendelő a fejlesztőt bízza meg a szoftver üzemeltetésével, aki a saját infrastruktúrája részeként üzemelteti azt, a megrendelő EIR-jének kell tekinteni, de a technikai kontrollok érvényre juttatás megoszlik a megrendelő és a fejlesztő között. A megrendelőnek a szükséges kiberbiztonsági követelményeket szerződéses kötelemként kell a fejlesztővel szemben érvényre juttatnia.

2. A VIZSGÁLANDÓ KÉRDÉS

Adott egy szoftver, amelyet egy fejlesztőcéggel termékként elad a megrendelő számára. A Megrendelő a Fejlesztőt bízza meg a szoftver üzemeltetésével, aki a saját infrastruktúrája részeként üzemelteti azt. A szoftver a megrendelő front office környezetének egyik elemeként működik.

3. VÁLASZ

Annak előre bocsátása mellett, hogy konkrét szoftverek esetében a szerződés és a vonatkozó dokumentáció ismeretében lehetséges választ adni az ilyen kérdésekre, a kérdésfeltevés szerinti elektronikus információs rendszer (EIR) jogilag a Megrendelőé, az ő „rendelkezésében lévő” rendszernek minősül, még akkor is, ha fizikailag a Fejlesztő infrastruktúráján fut és ő üzemelteti. A Magyarország kiberbiztonságáról szóló 2024. évi LXIX tv. (Kiberbiztonsági tv.) értelmében a nem a fizikai birtoklás vagy az üzemeltetés helye a döntő, hanem az, hogy kinek a tevékenységét támogatja a rendszer, és ki dönt az EIR alkalmazásáról és a benne kezelt adatokról. Mivel a szoftver a Megrendelő front office környezetének eleme és ő vásárolta meg, tehát ő az üzleti tulajdonos, a rendszer az ő rendelkezési körébe tartozik.

6. § (1) A szervezet elektronikus információs rendszerének kell tekinteni a szervezet rendelkezésében lévő elektronikus információs rendszert.

Ebben az esetben a Megrendelő a Kiberbiztonsági tv. alanya (a „Szervezet”), így neki kell gondoskodnia a rendszer védelméről, kockázatelemzéséről és biztonsági osztályba sorolásáról. A Fejlesztő ebben a felállásban közreműködőnek (és egyben kihelyezett szolgáltatónak) minősül. Mivel a Megrendelő bízta meg őt az üzemeltetéssel, a Fejlesztő a Megrendelő nevében és utasításai szerint jár el az infrastruktúra biztosítása során.

A törvény előírja, hogy a Megrendelő felelős azért, hogy a kiszervezett tevékenységek során is érvényesüljenek a biztonsági követelmények.

6. § (5) d) ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése [...] során, [...] gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek;

Bár jogilag az EIR a Megrendelőé, a technikai kontroll megoszlik. A 7/2024. (VI. 24.) MK rendelet kezeli az ilyen „osztott” helyzeteket:

- A megrendelő (Adatgazda) rendelkezik az adatok, a felhasználói jogosultságok, az üzleti logika és a szoftver funkciói felett. Ő határozza meg a biztonsági követelményeket (pl. biztonsági osztályba sorolás).
- A fejlesztő (Üzemeltető) rendelkezik az infrastruktúra (szerverek, hálózat, operációs rendszer) felett. Neki kell végrehajtania a Megrendelő által előírt védelmi intézkedéseket.

A jogszabály kimondja, hogy ha a rendelkezési jog korlátozott (pl. a szerver a Fejlesztőé), akkor a Megrendelőnek azokon a pontokon kell teljesítenie a követelményeket, amelyekre a joga kiterjed, a többit pedig szerződésben kell áthárítani (ld Kiberbiztonsági tv. 6. § (5) bek. d) pont).

2. § (3) Ha a szervezet rendelkezési joga az elektronikus információs rendszernek csak egyes elemeire vagy funkcióira terjed ki, a 2. mellékletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni.

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