

Milyen vonzatai vannak egy szerverbeszerzésnek NIS2-kötelezett vállalkozás esetén? Lehetséges-e használt szervert vásárolni?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi
állásfoglalás 2026/46

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.22	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Egy közép vállalat szerverbeszerzése a jog szemében nem egyetlen adásvétel, hanem négy, eltérően kezelendő elem együttese. A hardver és az alapszoftverek rendszerelemek, amelyekre a beszerzési követelmények vonatkoznak. A gyártói helyszíni garancia karbantartás és javítás, a tervezés, a beüzemelés és a migráció pedig a rendszer létrehozásához kötődő tevékenység. Mindhárom szállító közreműködő, de nem azonos súlyú. Az egyszeri termékszállító a rendszerhez nem fér hozzá, vele szemben a termékre vonatkozó szerződéses követelményeket kell érvényesíteni. A garanciális szerviz és a beüzemelő partner a rendszerben dolgozik, gyakran távolról, ezért rá a karbantartás és a személyi biztonság követelményei is vonatkoznak. Egyikük sem kihelyezett szolgáltató, amíg a szerződés nem foglal magában folyamatos üzemeltetést. A szervezet vezetője mindegyikért felelős marad.

A beszállítói kockázatelemzés minden biztonsági osztályban kötelező, és szerverbeszerzésnél konkrét kérdésekre keresi a választ. Meddig kap a platform firmware-frissítést, mennyi időn belül érkezik cserealkatrész, ki és hogyan fér hozzá a szerverhez a szerviz során, eredeti-e a hardver, és mi történik a meghibásodott adathordozóval. A válaszok adják a szerződés tartalmát.

Használt szerver vásárlását a szabályozás nem tiltja. A Rendelet a rendszerelem eredetiségét, a támogatás meglétét, a sérülékenységek javítását és a leltárba vételt várja el, és ezek újnál és használtnál azonosak, használt eszközénél azonban nehezebben teljesíthetők. Álláspontunk szerint a gyártói felújított, gyártói támogatással kísért szerver az újjal egyenértékű, a dokumentált eredetű használt szerver alap és jelentős osztályban kockázati döntés alapján beszerezhető, az ismeretlen eredetű, támogatás nélküli eszköz pedig kritikus szerepbe és magas osztályba nem való.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2¹-kötelezett közép vállalkozás (a továbbiakban mint „Szervezet”) kiöregedett szerverkörnyezetét cseréli. A beszerzés tárgya a fizikai szerver a tárolóval és a hálózati elemekkel, a hipervízor, a szerver operációs rendszerek és az adatbázis-kezelő licencei, a gyártói helyszíni garancia, valamint a rendszertervezés, a beüzemelés, a migráció, a mentési stratégia kialakítása és az oktatás. Feltételezzük, hogy a Szervezet a rendszert saját munkatársaival üzemelteti, üzemeltetési szerződést nem köt, ezért az állásfoglalás a kihelyezett üzemeltetéssel nem foglalkozik. Az ajánlatok között használt és felújított szerverek is szerepelnek. A vizsgálandó kérdések a következők.

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) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv), különösen a 21. cikk (2) bekezdés d) és e) pontja és (3) bekezdése.

- Milyen összetevőkből áll egy szerverbeszerzés, és hogyan illeszkednek ezek a szabályozás fogalmaiba?
- Közreműködőnek minősül-e a hardver, a szoftverkomponensek és a kapcsolódó szolgáltatások szállítója?
- Hogyan kell lefolytatni a beszállítói kockázatelemzést?
- Milyen kiberbiztonsági követelmények merülnek fel a beszerzés során, és mi legyen a szerződésben?
- Mire kell figyelni, ha a szállító nagy multinacionális cég?
- Vásárolható-e használt szerver?

A közreműködő és a kihelyezett szolgáltató elhatárolását [A közreműködő és kihelyezett szolgáltató fogalma és elhatárolása](#) című jogi állásfoglalás (2026/30), a közreműködői szerződések általános tartalmát [A közreműködővel kötött szerződés tartalma](#) című iránymutatás (2026/10) tárgyalja. Az ott leírtakat nem ismételjük, csak a szerverbeszerzés sajátosságaival foglalkozunk.

3. GYAKORLATI JAVASLATOK

3.1 A beszerzés összetevői és a rájuk vonatkozó fő követelmények

A táblázat a beszerzés tipikus elemeit, a szállító minősítését és a Rendelet² 2. mellékletének legfontosabb követelményeit foglalja össze, a biztonsági osztály megjelölésével.

Összetevő	Jellemző tartalom	A szállító minősítése	Fő követelmények
Hardver	rackszerver, processzor, memória, tároló, hálózati csatoló, tápegység, távoli felügyeleti vezérlő	rendszerem és IKT-termék szállítója, közreműködő rendszerhozzáférés nélkül	16.7. szerződéses követelmények, 16.15. dokumentáció, 19.23. eredetiség, 16.99. támogatás, 6.36. leltár (A, J, M); 16.13. portok és protokollok (J, M)
Alapszoftverek és licencek	hipervízor, szerver operációs rendszer, adatbázis-kezelő, mentőszoftver	IKT-termék gyártója, a viszonteladó a szerződő fél, közreműködő	16.8. védelmi funkciók leírása, 18.2. hibajavítás, 16.49. külső szolgáltatás a licenc- és támogatási portálokra, 6.23. konfigurációs beállítások (A, J, M)
Gyártói garancia és támogatás	következő munkanapos vagy négyórás helyszíni javítás, cserealkatrész, távoli diagnosztika	karbantartást és javítást végző közreműködő helyszíni és távoli hozzáféréssel	10.2. szabályozott karbantartás, 10.11. távoli karbantartás, 10.18. karbantartó személyek, 14.11. személyi biztonság, 19.7. alvállalkozók (A, J, M); 10.21. pótalkatrész-idő (J, M)
Tervezés, beüzemelés, migráció, mentés, oktatás	méretezés, rackbe építés, telepítés, adatátköltöztetés, mentési rend, betanítás	a rendszer létrehozásában részt vevő közreműködő, a migrációnál adatfeldolgozó is	16.7.8. felelősségmegosztás, 16.7.9. teljesítési kritériumok, 6.2. alapkonfiguráció, 6.15. biztonsági hatásvizsgálat, 7.35. mentések, 11.8. a régi adathordozók törlése (A, J, M); GDPR 28. cikk

² A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban Rendelet). Az „A”, „J”, „M” jelölés az „alap”, a „jelentős”, illetve a „magas” biztonsági osztályban kötelező, az „O” az egyik osztályban sem kötelező (opcionális) követelményt jelöl.

3.2 Használt szerver beszerzésének feltételei

Használt vagy felújított szerver akkor vehető, ha a Szervezet a beszerzés előtt a következőket tisztázza és dokumentálja.

- a) Az eredet ismert, a szállító igazolja a származást, a Szervezet a sorozatszámokat a gyártónál ellenőrzi, az alkatrészeket a gyártói konfigurációval összeveti.
- b) Támogatás rendelkezésre áll. A platform a tervezett életciklus alatt kap biztonsági firmware-frissítést, a letöltés jogosultsága a Szervezetnél van, lejáró támogatás esetén dokumentált alternatív támogatás szükséges.
- c) A szerviz és alkatrész ellátás biztosított, garancia vagy harmadik feles karbantartási szerződés a meghatározott időn belüli alkatrészcsere, vagy saját cserealkatrész-készlet.
- d) A szerver üzembe helyezése „gyári beállításokkal” tiszta állapotban történik. Ehhez szükséges a felügyeleti vezérlő és a BIOS gyári alaphelyzetbe állítása, a firmware újratelepítése hiteles gyártói forrásból, a jelszavak és tanúsítványok cseréje, a platformmodul törlése.
- e) Adathordozók és licencek ellenőrzése az érkező adathordozók cseréje vagy törlése a tartalom megismerése nélkül, a hardverhez kötött licencek átruházhatóságának ellenőrzése, az előfizetéses licencek beszerzése új jogosultként.
- f) Kockázati döntés, a beszerzés szerepel a kockázatelemzésben, a maradó kockázatot a Szervezet vezetője elfogadja, a használatbavételről jegyzőkönyvben dönt.

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 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.³ A közsférába tartozó, az 1. § (1) bekezdés a)-c) és f) pontja szerinti szervezetek eltéréseit az utolsó pont foglalja össze.

A szerverbeszerzés a törvény fogalmai szerint rendszerelemek beszerzése és az elektronikus információs rendszer (EIR) módosítása. A törvény a védelmet kifejezetten kiterjeszti az adatok kezelésére használt eszközökre, ideértve a hardvert és az adathordozókat, valamint az ezeket kezelő személyekre.⁴ A szervezet vezetőjének feladata a kockázatokkal arányos védelmi intézkedések meghatározása és a rendszer használatbavételéről szóló döntés,⁵ továbbá a közreműködőkkel szembeni követelmények szerződéses érvényesítése.⁶ A fejlesztésre vonatkozó hatósági eljárások⁷ a d) pont szerinti szervezetekre nem vonatkoznak, a részletes követelményeket számukra a Rendelet 2. mellékletének 6. (Konfigurációkezelés), 10.

³ 2024. évi LXIX. tv. 23. § (1) bekezdés b) pont

⁴ 2024. évi LXIX. tv. 5. § (2) bekezdés a)-c) pont

⁵ 2024. évi LXIX. tv. 6. § (3) bekezdés 6. és 12. pont

⁶ 2024. évi LXIX. tv. 6. § (5) bekezdés d) pont

⁷ 2024. évi LXIX. tv. 13. § (1) bekezdés és 14. § (1) bekezdés

(Karbantartás), 15. (Kockázatkezelés), 16. (Rendszer- és szolgáltatásbeszerzés) és 19. (Ellátási lánc kockázatkezelése) követelménycsoportja adja.

Középvállalatnál a serverbeszerzés négy rétegből áll, a fizikai infrastruktúrából, az alapszoftverek licenceiből, a gyártói hardvergaranciából és a kapcsolódó szolgáltatásokból. A garancia jellemzően három, öt vagy hét éves, következő munkanapos vagy négyórás helyszíni javítás, amelynél a gyártó vagy partnere mérnöke a cserealkatrészt hozza és beépíti, a szolgáltatások pedig a tervezéstől a telepítésen és a migráción át a mentési stratégia kialakításáig és a betanításig terjednek. A jog a négy réteget nem egyformán kezeli. A hardver és a szoftver a Rendelet szóhasználatában rendszerelem, a törvény szerint IKT-termék, amelynek gyártója a törvény értelmező rendelkezése szerinti „gyártó”.⁸ A garancia karbantartás és javítás, a beüzemelés és a migráció a rendszer létrehozásához kapcsolódó tevékenység. A közreműködői minősítés és a szerződés tartalma a tevékenység jellegéhez igazodik, nem a számla tételéhez. A beszerzés ötödik, gyakran elfelejtett eleme a régi server kivezetése a migráció végén.⁹

4.2 **Ki minősül közreműködőnek?**

A törvény a közreműködőt nem definiálja, hanem tevékenységeken keresztül írja körül.

d) ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, illetve a kiberbiztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási tevékenység ellátásához, 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; [2024. évi LXIX. törvény 6. § (5) bekezdés d) pont]

A 2026/30. számú állásfoglalás (<https://nis2.mkik.hu/jogi-allasfoglalasok/30>) ebből vezette le, hogy a közreműködő funkcionális fogalom, és hogy a szoftver- és hardverbeszállítók közreműködőnek minősülnek, kihelyezett szolgáltatónak azonban nem. A serverbeszerzés három szállítói szerepére ezt az alábbiak szerint pontosítjuk.

A *hardver szállítója* a rendszer létrehozásához szükséges rendszerelemet adja, ezért közreműködő. A tisztán termékszállító azonban a Szervezet rendszeréhez nem fér hozzá, adatot nem kezel. A törvény az „ellátott tevékenységgel összefüggésben szükséges” követelmények érvényesítését várja el, ezért a termékszállítóra a rendszerhozzáféréssel járó követelmények nem vonatkoznak, a termék tulajdonságait a beszerzési szerződés követelményei fedik le.¹⁰ Ha

⁸ 2024. évi LXIX. tv. 4. § 32. és 39. pont; az IKT-termék fogalmát a törvény az (EU) 2019/881 rendelet 2. cikk 12. pontjára utalással határozza meg.

⁹ A régi eszközök adathordozóinak törlését és a leltár lezárását a PC-k és notebookok selejtezéséről és értékesítéséről szóló korábbi állásfoglalásunk tárgyalja, az ott leírtak a szerverre is irányadók.

¹⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.7. pont

ugyanaz a szállító a garanciát és a beüzemelést is adja, a minősítése a legmagasabb hozzáférésű tevékenységéhez igazodik.

A szoftverkomponensek szállítója. A hipervizor, az operációs rendszer és az adatbázis-kezelő gyártója IKT-termék gyártója, a Szervezet szerződő partnere pedig többnyire a viszonteladó. A szoftver hibái a rendszer sérülékenységei, ezért a gyártó a rendszer létrehozásában és karbantartásában akkor is részt vesz, ha a Szervezettel közvetlenül nem szerződik. A követelményeket a viszonteladóval kötött szerződésben és a gyártói licencfeltételek beépítésével kell érvényesíteni. A támogatási előfizetés távoli diagnosztikája karbantartás,¹¹ a licenc- és támogatási portálok, a felhőalapú aktiválás és a telemetria pedig külső elektronikus információs rendszer szolgáltatásai.¹²

A kapcsolódó szolgáltatások nyújtója. A garanciális szerviz karbantartást és javítást végez, a beüzemelő és a migrációt végző partner a rendszer létrehozásában vesz részt, közreműködői minőségük nem kérdéses. A rendszerben dolgoznak, helyszínen és távolról, adminisztrátori jogosultsággal, a migráció során személyes adatokkal is, ezért rájuk a karbantartó személyekre,¹³ a külső személyek személyi biztonságára¹⁴ és az adatfeldolgozói szerződésre vonatkozó szabályok is vonatkoznak.¹⁵ A kihelyezett (irányított) szolgáltató törvényi meghatározása¹⁶ a telepítést és a karbantartást is említi, a 2026/30. számú állásfoglalás szerint azonban a minősítés a tartós, irányított szolgáltatásnyújtáshoz kötődik, ezért egyikük sem kihelyezett szolgáltató, amíg tevékenységük eseti, és nem terjed ki a rendszer folyamatos üzemeltetésére vagy felügyeletére. A gyártói garancia akkor sem üzemeltetés, ha a szerver automatikus hibajelzést küld a gyártónak. Ha viszont a Szervezet a garanciával együtt folyamatos távfelügyeleti szolgáltatást is vásárol, a 2026/30. számú állásfoglalás szerinti elhatárolást el kell végezni. Az elektronikus információs rendszer biztonságáért felelős személy mindhárom közreműködőtől jogosult tájékoztatást és dokumentumokat kérni,¹⁷ ezt a jogot a szerződésben célszerű nevesíteni.

4.3 A beszállítói kockázatelemzés

A rendszerszintű kockázatelemzés minden osztályban kötelező, és a Rendelet külön nevesíti az ellátási láncot. A Szervezet felméri az ellátási lánc kockázatait a rendszerelemei és rendszerszolgáltatásai vonatkozásában, és a kockázatelemzést jelentős változás esetén frissíti.¹⁸ A szerverbeszerzés ilyen változás, ezért a kockázatelemzést a beszerzés előtt kell frissíteni, nem utána. A kereteket az ellátási lánc kockázatmenedzsment szabályzata adja, amely a beszerzés, a szállítás, az integráció, az üzemeltetés és karbantartás, valamint a kivezetés szakaszait fedi le.¹⁹ A fenyegetéseket a Rendelet 3. mellékletének katalógusából kell azonosítani, ahol a beszállítói

¹¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.11. pont (A, J, M)

¹² 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.49. pont (A, J, M)

¹³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.18. pont (A, J, M)

¹⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.11. pont (A, J, M)

¹⁵ Az (EU) 2016/679 rendelet (GDPR) 28. cikk (3) bekezdése az adatfeldolgozói szerződés kötelező tartalmát írja elő (tartalmi összefoglalás).

¹⁶ 2024. évi LXIX. tv. 4. § 52. és 53. pont

¹⁷ 2024. évi LXIX. tv. 11. § (9) bekezdés

¹⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 15.5. pont (A, J, M)

¹⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.2. pont (A, J, M)

lánc megszakadása, a külső szolgáltatók hibája, a hardver vagy szoftver hamisítása és a szoftverek sérülékenységei külön tételként szerepelnek.²⁰ Jelentős és magas osztályban a kritikus rendszerelemeket kritikussági elemzéssel kell azonosítani,²¹ a beszállítókat pedig meghatározott gyakorisággal felül kell vizsgálni.²² A serverbeszerzés sajátos kockázati kérdései a következők.

- a) Támogatási horizont. Meddig ad a gyártó biztonsági firmware-frissítést, és ez lefedi-e a tervezett öt-hét éves életciklust. A támogatás megszűnése után csere vagy alternatív támogatás szükséges.²³
- b) Alkatrész-ellátás és javítási idő. Jelentős és magas osztályban a Szervezet határozza meg, milyen időn belül kell cserealkatrészt biztosítani.²⁴ A garancia szintje ebből következik, nem fordítva.
- c) Hozzáférés és adathordozók a szerviz során. Ki, milyen csatornán és jogosultsággal fér hozzá a rendszerhez, hogyan hagyja ezt jóvá a Szervezet, és mi lesz a meghibásodott lemezzel, amelyet az elszállítás előtt törölni kell.²⁵
- d) Eredetiség. Hivatalos csatornán érkezik-e az eszköz és minden alkatrésze, és a Szervezet hogyan ellenőrzi átvételkor a hamisítást.²⁶
- e) Függőség és alvállalkozói lánc. A környezet egyetlen gyártóra és szervizpartnerre épül, a helyszíni szerviz és a beüzemelés jellemzően alvállalkozó. A diverzifikált beszállítói bázis opcionális,²⁷ a követelmények továbbhárítása az alvállalkozókra kötelező.²⁸ A migráló partner adatkezelése és a használt eszköz eredetisége, támogatása és adathordozói külön értékelendők.

Az eredményt a kockázatelemzési jelentésben kell dokumentálni,²⁹ a beszerzési stratégiát és a szerződéses eszközöket a kockázatokhoz kell igazítani,³⁰ a használatbavételről pedig a vezető jegyzőkönyvben dönt.³¹ A közszférába tartozó szervezetek az Európai Bizottság és az ENISA kritikus ellátási láncokra vonatkozó összehangolt kockázatértékeléseit is figyelembe veszik,³² ezt magánvállalkozásnak is javasoljuk a gyártó székhelye szerinti joghatóság és a geopolitikai kitettség értékelésénél.

²⁰ 7/2024. (VI. 24.) MK rendelet 3. melléklet 1. pont, a fenyegetéskatalógus táblázatának 11., 12., 22. és 29. sora

²¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 15.21. pont (J, M)

²² 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.16. pont (J, M)

²³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.99. pont (A, J, M)

²⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.21. pont (J, M)

²⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.2.4. pont (A, J, M)

²⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.22. és 19.23. pont (A, J, M)

²⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.5. pont (O)

²⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.7. pont (A, J, M)

²⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 15.4.3. pont (A, J, M)

³⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.13. pont (A, J, M)

³¹ 7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.6. pont

³² 418/2024. (XII. 23.) Korm. rendelet 4. § (1) bekezdés, amely az 1. § (1) bekezdés szerint a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) és f) pontja szerinti szervezetekre alkalmazandó.

4.4 Kiberbiztonsági követelmények a beszerzés során és a szerződésben

Minden osztályban kötelező a beszerzési szabályzat és eljárásrend,³³ amelynek közép vállalatnál nem kell külön dokumentumnak lennie, a meglévő beszerzési szabályzat információbiztonsági fejezete is megfelel. A biztonságot a beruházás tervezésekor elkülönített tételként kell kezelni,³⁴ ami szervernél a felügyeleti vezérlő biztonsági licencét, a mentési célrendszert, a redundanciát és a garancia szintjét jelenti. A szerződéses követelmények minimumát a Rendelet tételesen adja.

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:

16.7.1. A funkcionális biztonsági követelményeket.

[...]

16.7.4. Az érintett EIR biztonsági osztályát és az ahhoz tartozó, illetve a szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedéseket.

16.7.5. A biztonsággal kapcsolatos dokumentációs követelményeket.

[...]

16.7.8. A felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását.

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

A szerverbeszerzésnél egyetlen keretben négy jogviszony jelenik meg, adásvétel, licencszerződés, garanciális szolgáltatás és vállalkozási szerződés, és a követelményeket mindegyikhez a saját tárgya szerint kell hozzárendelni. A szoftverlicenceknél a licenc átruházhatósága, a támogatás lejárata, a frissítések elérhetősége és a gyártóhoz kimenő adatok köre rögzítendő. Az iránymutatás (2026/10) általános elemein felül a következőket javasoljuk.

A hardver adásvételénél a szerződés a termék tulajdonságairól szól. A pontos konfiguráció és a sorozatszámok, az új és eredeti állapot vagy a felújítás ténye, a szállítási csatorna és az átvételi ellenőrzés a hamisított rendszerelemek kizárására szolgáló eljárás³⁵ szerződéses vetületei. A támogatás lejárata és a firmware-frissítések elérhetősége a támogatás nélküli rendszerelemek cseréjének³⁶ és a firmware-frissítések határidős telepítésének³⁷ feltétele. A biztonsági konfigurációs útmutató és az adminisztrátori dokumentáció,³⁸ valamint a portok és protokollok listája³⁹ a Rendelet szerinti dokumentáció, magas osztályban a szállítás már a meghatározott

³³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.1. pont (A, J, M)

³⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.2. pont (A, J, M)

³⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.23. pont (A, J, M)

³⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.99. pont (A, J, M)

³⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 18.2.3. pont (A, J, M)

³⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.8. és 16.15. pont (A, J, M)

³⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.13. pont (J, M)

biztonsági konfigurációval történik.⁴⁰ A sérülékenységi értesítés módja és határideje a Rendelet szerinti értesítési megállapodás,⁴¹ amelyet a gyártó nyilvános közleményeire történő feliratkozás önmagában nem pótol.

A *garanciánál* a szerződés a hozzáférésről szól. A reakció- és javítási időt órában kell megadni, mert jelentős és magas osztályban a Szervezet határozza meg az alkatrész-biztosítás idejét.⁴² A helyszíni mérnök azonosítása, kíséréte és személyi biztonsági megfelelése⁴³ szerződéses kérdés. A távoli diagnosztika csatornáját le kell írni, a rendszerbiztonsági tervben dokumentálni és minden alkalommal jóváhagyni kell,⁴⁴ az automatikus hibajelentés bekapcsolása ezért tudatos döntés. A meghibásodott adathordozó helyben tartása a törlési kötelezettség⁴⁵ teljesítésének legegyszerűbb módja, a nagy gyártók ezt külön, a garancia megrendelésekor választható opcióként kínálják. A szervizpartner alvállalkozói minőségét a követelmények alvállalkozókra való továbbhárítása miatt kell rögzíteni.⁴⁶

A *beüzemelésnél és a migrációnál* a teljesítési kritériumok⁴⁷ a legfontosabbak. Átadási feltétel a legkorlátozottabb üzemmódot képviselő biztonsági alapkonzfiguráció a felügyeleti vezérlőn, a BIOS-on, a hipervizoron és az operációs rendszeren,⁴⁸ a dokumentáció, a mentés⁴⁹ és a visszaállítás sikeres tesztje,⁵⁰ a leltár és a rendszerbiztonsági terv frissítése,⁵¹ a változtatás biztonsági hatásvizsgálata.⁵² A partner adminisztrátori hozzáférését a szerződés ideiglenesnek nyilvánítja, átadáskor visszavonja, a hitelesítő eszközöket visszaveszi.⁵³ A migrált adatokra adatfeldolgozói klauzula szükséges, a régi szerver adathordozóinak törlését és igazolását pedig a szerződésbe kell építeni, ha azt a partner végzi.⁵⁴ A szerződés az információbiztonságért felelős feleket azonosítja,⁵⁵ a Szervezet vezetőjének felelőssége azonban a garanciából sem tűnik el.⁵⁶

A megfelelés igazolására tanúsított IKT-termék használható, ha rendelkezésre áll, kötelező pedig csak akkor, ha az SZTFH elnökének rendelete az adott szervezeti körre és termékre előírja.⁵⁷ A gyártói oldalon az uniós kiberrezilienciáról szóló jogszabály 2027 decemberétől a szervezetre is biztonsági alapkövetelményeket és támogatási időszakot ír elő, a gyártók aktívan kihasznált

⁴⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.11. pont (M)

⁴¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.19. pont (A, J, M)

⁴² 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.21. pont (J, M)

⁴³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.18. és 14.11. pont (A, J, M)

⁴⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.11. pont (A, J, M)

⁴⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.2.4. pont (A, J, M)

⁴⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.7. pont (A, J, M)

⁴⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.7.9. pont

⁴⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.2. és 6.23. pont (A, J, M)

⁴⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 7.35. pont (A, J, M)

⁵⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 7.36. pont (J, M)

⁵¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.36. pont (A, J, M)

⁵² 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.15. pont (A, J, M)

⁵³ A hitelesítő eszközök kiadását és visszavonását a hitelesítő eszközök nyilvántartásáról szóló 2026/33. számú állásfoglalás tárgyalja.

⁵⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 11.8. pont (A, J, M)

⁵⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.7.8. pont

⁵⁶ 2024. évi LXIX. tv. 6. § (6) bekezdés

⁵⁷ 2024. évi LXIX. tv. 6. § (8) és (9) bekezdés

sérülékenységekre vonatkozó bejelentési kötelezettsége pedig 2026. szeptember 11. óta él,⁵⁸ ezért a gyártó megfeleléségi ütemtervére és támogatási időszakára már ma érdemes rákérdezni.

4.5 **Ha a szállító nagy multinacionális gyártó**

A nagy gyártók gyakorlata három ponton tér el a hazai partnerektől. Az általános szerződési és garanciafeltételeik alig tárgyalhatók, a szerződő fél többnyire nem a gyártó, hanem a hazai disztribútor vagy viszonteladó, a támogatási folyamatok pedig globálisak, a hibajegyek és a diagnosztikai adatok az Európai Gazdasági Térségen kívülre is eljuthatnak. A követelményeket a viszonteladóval kötött szerződésben kell érvényesíteni, a gyártói feltételeket mellékletként kezelni, és rendezni, hogy ellentmondás esetén melyik érvényesül. A viszonteladó a termék tulajdonságaira a gyártói feltételeken túl nem vállal kötelezettséget, tud viszont a szállítási csatornára, az átvételi ellenőrzésre, a dokumentációra, a helyi szervizpartnerre és az értesítésekre. A magyar jog és fórum kikötése a kikényszeríthetőség miatt javasolt.

A gyártói dokumentáció ebben a helyzetben bizonyíték. A nagy gyártók nyilvános biztonsági konfigurációs útmutatói, termékbiztonsági közleményei, támogatási és életciklus-politikái, valamint a platformba épített, a szállítási lánc sértetlenségét igazoló eredetiség-ellenőrző megoldásaik a dokumentációs, támogatási és eredetiségi követelmények teljesítésének dokumentumai.⁵⁹ A Szervezet ezeket a beszerzési aktában gyűjti, és a beszállító jelentős és magas osztályban kötelező felülvizsgálatát⁶⁰ ezek alapján végzi, 2027 decemberétől a kiberrezilienciáról szóló jogszabály szerinti megfeleléségi nyilatkozattal együtt.

A gyártók távoli támogatási és flottafelügyeleti platformjai, az automatikus hibajelentés és a telemetria a gyártó felhőjébe küld adatot. Ezek a Szervezet szempontjából külső elektronikus információs rendszer szolgáltatásai,⁶¹ amelyek bekapcsolása előtt a kimenő adatok körét, a tárolás helyét és a hozzáférés jogosultjait tisztázni kell, személyes adat esetén a harmadik országba irányuló adattovábbítás szabályaival együtt.⁶² A geopolitikai és joghatósági kockázat a kockázatelemzés része. Az Európai Bizottság, a tagállamok és az ENISA 2026 februárjában közzétett IKT ellátási lánc biztonsági eszköztára a kritikus beszállítók értékeléséhez és a magas kockázatú beszállítóktól való függés kezeléséhez ad módszertant, a kiberbiztonsági jogszabály felülvizsgálata pedig megbízható IKT ellátási lánc keretrendszer javasol.⁶³ A közsférában az uniós összehangolt kockázatértékelések figyelembevétele kötelező, magánvállalkozásnál a kockázatelemzés alaposságának mércéje.

⁵⁸ Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (kiberrezilienciáról szóló jogszabály) 13. és 14. cikk; a bejelentési kötelezettség 2026. szeptember 11-től, a többi kötelezettség 2027. december 11-től alkalmazandó (tartalmi összefoglalás).

⁵⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.8., 16.15., 16.99. és 19.23. pont (A, J, M)

⁶⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.16. pont (J, M)

⁶¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.49. pont (A, J, M)

⁶² GDPR V. fejezet (44-49. cikk) és 28. cikk; az Európai Adatvédelmi Testület 05/2021. számú iránymutatása és 01/2020. számú ajánlása (tartalmi összefoglalás).

⁶³ NIS Cooperation Group, EU ICT Supply Chain Security Toolbox, 2026. február 13.; az Európai Bizottság 2026. január 20-i javaslata az (EU) 2019/881 rendelet felülvizsgálatára (tartalmi összefoglalás).

4.6 Lehetséges-e használt szervert vásárolni?

Sem a Kiberbiztonsági tv., sem a Rendelet nem írja elő, hogy a rendszerelemnek újnak kell lennie. A Rendelet eredetiséget, támogatottságot, javított sérülékenységeket és dokumentált konfigurációt vár el a beszerzés módjától függetlenül. A használt szerver tehát jogilag beszerezhető, a kérdés az, hogy a követelmények használt eszközknél teljesíthetők-e, és milyen áron. Az első követelmény az eredetiség.

19.23. A szervezet:

19.23.1. kialakítja és bevezeti a hamisítás elleni szabályokat és eljárásokat, amelyek magukban foglalják a hamisított rendszerelemek észlelését és annak megelőzését, hogy ezek bejussanak az EIR-be; valamint

[...] [7/2024. (VI. 24.) MK rendelet 2. melléklet 19.23. pont] (A, J, M)

Új eszközknél a hivatalos csatorna és a gyártói zárócímke az ellenőrzés alapja. Használt eszközknél a lánc megszakad, az alkatrészek cserélhetők, a firmware módosítható. A Szervezetnek ezért a származást igazoltatnia, a sorozatszámokat a gyártónál ellenőriznie, az alkatrészeket a gyártói konfigurációval egyeztetnie, és a rendszert használatbavétel előtt hamisítás szempontjából megvizsgálnia kell.⁶⁴ Ezt a legmegbízhatóbban a firmware újratelepítése hiteles gyártói forrásból és a felügyeleti vezérlő gyári alaphelyzetbe állítása adja, mert a korábbi tulajdonos fiókjai és tanúsítványai a vezérlőben maradnak.

A második a támogatás. A támogatás nélküli rendszerelemet a Szervezet lecseréli vagy alternatív támogatást biztosít hozzá,⁶⁵ a biztonsági firmware-frissítéseket pedig meghatározott időn belül telepíti.⁶⁶ A használt szerver jellemzően korábbi generáció, amelynek gyártói támogatása rövidebb ideig tart, a frissítések letöltése egyes gyártóknál aktív támogatási szerződéshez kötött, az újabb hipervizor-verziók pedig a régebbi processzorokat kivezetik, ezért a tervezett életciklust a maradék támogatási időhöz kell igazítani. A harmadik feles karbantartás az alkatrészcsere megoldja, a firmware biztonsági javításait nem pótolja.⁶⁷

A harmadik az adathordozók kérdése. A használt szerverrel érkező lemezekon a korábbi tulajdonos adatai maradhettek, ezeket a Szervezet nem jogosult megismerni, az adathordozókat ezért a tartalom vizsgálata nélkül törli vagy cseréli, és a törlést dokumentálja.⁶⁸ Gyártói garancia hiányában a szerviz során meghibásodott lemez törléséről⁶⁹ a Szervezetnek magának kell gondoskodnia. A korlátozott élettartam miatt a használt szerverhez is új adathordozókat javaslunk.

⁶⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.22. pont (A, J, M)

⁶⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.99. pont (A, J, M)

⁶⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 18.2.3. pont (A, J, M)

⁶⁷ A támogatás nélküli rendszerelemek megtartásának feltételeit a nem támogatott operációs rendszerekről szóló korábbi állásfoglalásunk tárgyalja.

⁶⁸ A korábbi tulajdonos adatainak megismerése jogalap nélküli adatkezelés lenne, lásd a GDPR 5. cikk (1) bekezdés a) és f) pontját (tartalmi összefoglalás); a törlésre a Rendelet 2. melléklet 11.8. pontja (A, J, M) irányadó.

⁶⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.2.4. pont (A, J, M)

A negyedik a licencek és a szavatosság. A hardverhez kötött gyártói operációsrendszer-licenc az eszközzel együtt átruházható lehet, a mennyiségi és az előfizetési licencek jellemzően nem. Az uniós bíróság a használt szoftverlicencek továbbértékesítését meghatározott feltételekkel elismerte,⁷⁰ a licencfeltételek egyedi ellenőrzése nélkül azonban a használt szerverrel érkező szoftver nem használható. Vállalkozások között a kellékszavatossági igény egy év alatt évül el, és a felek a szavatosságot szűkíthetik,⁷¹ a használt szerverhez ezért a gyártói garancia helyett a szállító szavatossága vagy harmadik feles szervizszerződés tartozik, jelentős és magas osztályban a Szervezet által meghatározott alkatrész-biztosítási idővel.⁷²

Mindezek alapján álláspontunk a következő. A gyártói felújított, teljes gyártói garanciával és támogatással kísért szerver az újjal egyenértékű beszerzés, a különbség az életkor és a maradék támogatási idő. A hivatalos partnertől származó, dokumentált eredetű használt szerver alap és jelentős osztályban a fenti feltételekkel és a vezető által jóváhagyott kockázati döntéssel beszerezhető. Az ismeretlen eredetű, támogatás nélküli használt szervert kritikus rendszerelemként vagy magas osztályba sorolt rendszerhez nem javasoljuk, mert az eredetiség és a támogatás követelménye ilyenkor csak helyettesítő intézkedésekkel tartható. A vételár előnyét a firmware újratelepítése, az adathordozók cseréje, a szervizszerződés és a rövidebb életciklus rendszerint jelentősen csökkenti, ezért a döntést a teljes életciklus költségére kell alapozni.

5. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS 2 irányelv)
- Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (kiberbiztonsági jogszabály) és az Európai Bizottság 2026. január 20-i felülvizsgálati javaslata
- Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (kiberrezilienciáról szóló jogszabály)
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR); az Európai Adatvédelmi Testület 05/2021. számú iránymutatása és 01/2020. számú ajánlása
- 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
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.)
- Az Európai Unió Bírósága C-128/11. sz. UsedSoft ügyben hozott ítélete

⁷⁰ Az Európai Unió Bírósága C-128/11. sz. UsedSoft kontra Oracle ügyben 2012. július 3-án hozott ítélete (tartalmi összefoglalás).

⁷¹ 2013. évi V. törvény (Ptk.) 6:163. § (1) bekezdés; az eltérés lehetőségére a Ptk. 6:59. § (2) bekezdése irányadó (tartalmi összefoglalás).

⁷² 7/2024. (VI. 24.) MK rendelet 2. melléklet 10.21. pont (J, M)

- NIS Cooperation Group, EU ICT Supply Chain Security Toolbox (2026. február 13.)
- MKIK NIS2 Portál, A közreműködő és kihelyezett szolgáltató fogalma és elhatárolása (jogi állásfoglalás 2026/30); A közreműködővel kötött szerződés tartalma (iránymutatás 2026/10)