Egy külföldi székhelyű anyavállalat által üzemeltetett ERP-t fel kell -e venni az EIR-ek közé?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/1

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.26	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Azt hogy egy külföldi anyavállalat által üzemeltetett ERP rendszert (pl. SAP) minden esetben fel kell -e venni az elektronikus információs rendszerek (EIR) nyilvántartásába, az határozza meg, hogy melyik szervezeté a rendelkezési jog.

A rendelkezési jog a rendszer feletti tényleges kontrollt és döntési jogosultságot jelenti (üzemeltetés, konfiguráció, felhasználókezelés, továbbfejlesztés stb).

Amennyiben a magyar leányvállalatnak nincs rendelkezési joga a rendszer felett, azt nem szervezet saját rendelkezésében lévő EIR-ként, hanem a szervezet által igénybe vett külső elektronikus információs rendszer szolgáltatásként kell nyilvántartani. Ebben az esetben nem kell biztonsági osztályba sorolni, de a védelmi követelményeket itt is biztosítani kell szerződéses kötelezettségek formájában.

Részleges rendelkezési jog is előfordulhat. Ha a leányvállalat jogosult a konfigurációra és a felhasználók kezelésére, de az üzemeltetés az anyavállalat feladata, a rendszer alkalmazás-szinten saját rendelkezésűnek minősül. Ekkor kötelező a biztonsági osztályba sorolás, a helyi kontrollokat (jogosultságok, beállítások) pedig az auditor közvetlenül vizsgálja.

Bár a központi infrastruktúra (szerverek) kivonható a közvetlen technikai audit alól, a kliens oldali védelem, a hálózati kapcsolat és a beszállítói kockázatelemzés minden esetben az audit részét képezi.

2. A VIZSGÁLANDÓ KÉRDÉS

Külföldi székhelyű anyavállalat által előírt és üzemeltetett ERP rendszert (pl. SAP) fel kell-e venni az EIR-ek közé? Ha igen milyen osztályba kell besorolni? Ha nem, kivonható-e a kiberbiztonsági audit hatálya alól.

3. VÁLASZ

3.1 A rendelkezési jog fogalma

A kérdés megválaszolásának kulcsa a rendelkezési jog és a használat közötti jogi különbségtétel. A Kiberbiztonsági tv. különbséget tesz a szervezet saját rendszerei és az általa igénybe vett szolgáltatások között, azonban mindkettőt fel kell mérni.

A rendelkezési jog (*rendelkezésben lévő*) azt jelenti, hogy a szervezet jogi és technikai értelemben döntési jogkörrel bír a rendszer életciklusa, biztonsági paraméterei, üzemeltetése és fejlesztése felett. Ha az anyavállalat írja elő, üzemelteti, frissíti az ERP-t, és a magyar leányvállalat csak felhasználói hozzáféréssel bír (kliens oldali elérés), akkor a rendszer nincs a magyar szervezet rendelkezési körében.

A rendelkezési jog a kiberbiztonsági jogszabályok alkalmazásában nem csupán a tulajdonjogot jelenti, hanem a rendszer feletti tényleges kontrollt és döntési jogosultságot. Ez a fogalom

határozza meg, hogy egy szervezetnek milyen mélységű kötelezettségei vannak: a rendszert biztonsági osztályba kell sorolnia (ha rendelkezik felette), vagy csak nyilvántartásba kell vennie és szerződésesen szabályoznia (ha csak használja).

A fogalom pontos megértéséhez a 2024. évi LXIX. törvény (Kibertv.) és a kapcsolódó végrehajtási rendeletek logikáját, valamint a gyakorlati ismérveket kell megvizsgálni.

A Kibertv. nem tartalmaz külön „rendelkezési jog" definíciót az értelmező rendelkezések között, de a 6. § egyértelműen különbséget tesz a „rendelkezésben lévő" és a „használt" rendszerek között.

> *„A szervezet elektronikus információs rendszerének kell tekinteni a szervezet rendelkezésében lévő elektronikus információs rendszert."[2024. évi LXIX. törvény 6. § (1) bekezdés]*

A Kiberbiztonsági tv. szabályai (5. §) alapján az elektronikus információs rendszerek védelme az adott szervezet által az adatok, információk kezelésére használt eszközökre (ideértve a környezeti infrastruktúrát, a hardvert, a hálózatot és az adathordozókat), eljárásokra (ideértve a szabályozást, a szoftvert és a kapcsolódó folyamatokat) is kiterjed.

> *„Az elektronikus információs rendszer védelme keretében az elektronikus információs rendszer felett rendelkezési jogosultsággal rendelkező szervezet, az adatkezelő vagy az adatfeldolgozó által, adott cél érdekében*
> *a) az adatok, információk kezelésére használt eszközök, ideértve a környezeti infrastruktúrát, a hardvert, a hálózatot és az adathordozókat*
> *b) az adatok, információk kezelésére használt eljárások, ideértve a szabályozást, a szoftvert és a kapcsolódó folyamatokat, valamint*
> *c) az a) és b) pontban foglaltakat kezelő személyek*
> *együttesének védelmét is biztosítani szükséges." [2024. évi LXIX. törvény 5. § (2) bekezdés]*

Ez azt jelenti, hogy a törvény teljes szigora (pl. biztonsági osztályba sorolás, konkrét védelmi intézkedések auditálható megvalósítása) csak azokra a rendszerekre vonatkozik, amelyek felett a szervezet rendelkezési jogot gyakorol.

A gyakorlatban akkor beszélünk rendelkezési jogról, ha a szervezet (vagy az általa megbízott üzemeltető) képes érdemben befolyásolni a rendszer életciklusát, konfigurációját és biztonsági szintjét.

A rendelkezési jog három fő pilléren nyugszik:

A) Technikai kontroll (Üzemeltetés)

A rendszer felett rendelkezési joga van a szervezetnek, ha:

- Adminisztrátori joga van, azaz a szervezet (vagy helyi rendszergazdája) rendelkezik a legmagasabb szintű hozzáféréssel (pl. root, domain admin).
- Konfigurációs joga van, azaz szervezet döntheti el, milyen biztonsági beállításokat alkalmaz, milyen portokat nyit meg, milyen logolást állít be.

- Frissítések menedzsmentje az ő felelőssége, azaz a szervezet dönt a patch-ek telepítésének idejéről és módjáról.

B) Döntési kontroll

Nem feltétel a saját tulajdonú hardver, de feltétel a döntési autonómia:

- Életciklus-döntés, a szervezet döntheti el, hogy bevezeti, módosítja vagy kivezeti a rendszert.
- Változáskezelés, a szervezet jóváhagyása szükséges a rendszer lényegi módosításaihoz.

C) Jogi/felelősségi kontroll

- Adatgazda vs. Rendszergazda, fontos különbség, hogy az adatok felett jellemzően van rendelkezési joga a szervezetnek (adatkezelő), de a rendszer (az infrastruktúra és szoftver) felett nem feltétlenül.

Az alábbi táblázat segít eldönteni, hogy egy adott rendszer (pl. az anyavállalati SAP) melyik kategóriába esik:

Szempont	**Rendelkezésben lévő rendszer**	**Használt / Igénybe vett rendszer (pl. Anyavállalati szolgáltatás, SaaS)**
Példa	Helyi szerveren futó fájlszerver, saját fejlesztésű szoftver.	Microsoft 365 felhő ahol az anyavállalat a tenant admin, anyavállalati központi SAP.
Kiberbiztonsági feladat	Biztonsági osztályba sorolás (Alap/Jelentős/Magas).	Belső nyilvántartásba vétel (mint külső szolgáltatás).
Védelmi intézkedések	A szervezetnek kell megvalósítania (pl. 7/2024 MK rendelet szerint).	A szervezetnek szerződéses feltételként meg kell követelnie a szolgáltatótól (SLA, szerződés).
Hozzáférés szintje	Rendszergazdai (hozzáférés az OS-hez, adatbázishoz).	Felhasználói / Kulcsfelhasználói (csak az alkalmazás felületét éri el).
Audit tárgya	A rendszer technikai beállításait közvetlenül vizsgálják.	A szolgáltatói szerződést és a kapcsolódó kockázatkezelést vizsgálják részleges rendelkezési jog esetén.

Ha az anyavállalat adja a "dobozos" szolgáltatást (ők üzemeltetik a szervereket, ők végzik a mentést, ők állítják be a jelszóházirendet globálisan), akkor a magyar leányvállalatnak nincs rendelkezési joga a rendszer felett.

Ebben az esetben a magyar szervezet „csak” szolgáltatás-igénybevevő. Az ERP rendszert fel kell venni az elektronikus információs rendszerek (EIR) nyilvántartásába, de nem mint „rendelkezésben lévő” saját rendszert, hanem mint a szervezet által használt igénybe vett külső

szolgáltatást (amennyiben az anyavállalat belső szolgáltatóként vagy kiszervezett formában nyújtja). A nyilvántartásnak tükröznie kell, hogy ez egy külső, nem a szervezet által üzemeltetett rendszer.

Lényeges továbbá, hogy ha a rendelkezési jog bármely elemét az anyavállalat (vagy bármely egyéb szervezet) gyakorolja, akkor a szervezet közreműködőjének minősül a Kibertv. 6. § (5) bekezdés d) pont értelmében biztosítania kell, hogy a közreműködő által az EIR-el kapcsolatosan ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági követelmények szerződéses kötelemként teljesüljenek. Ezen kötelezettség teljeüsléséről az auditon számot kell adni a vonatkozó szerződés bemutatásával.

3.2 Mi a teendő ha a rendelkezési jog megoszlik?

Pl a külföldi anyavállalat üzemelteti az rendszert saját infrastruktúráján, de a magyar leányvállalat jogosult a rendszer konfigurálásásra és a felhasználó menedzsmentjére?

A megosztott rendelkezési jog esete a leggyakoribb és egyben a legkomplexebb szituáció a multinacionális környezetben működő leányvállalatoknál. Ebben az esetben a „rendszer” nem egy monolitikus egység, hanem rétegekre bomlik, és a jogi megfelelés kulcsa a felelősségi körök pontos elhatárolása.

A 7/2024. (VI. 24.) MK rendelet kifejezetten rendezi ezt a helyzetet:

> *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. [7/2024. (VI. 24.) MK rendelet 2. § (3) bekezdés]*

Amennyiben a magyar leányvállalat jogosult a rendszer konfigurálására (pl. üzleti logika, paraméterezés) és a felhasználók menedzsmentjére, akkor a rendszer – az alkalmazás szintjén – a szervezet rendelkezésében lévőnek minősül.

A Kibertv. fogalomrendszere alapján az elektronikus információs rendszer (EIR) nem csak a hardvert jelenti, hanem az eljárásokat, szoftvereket és adatokat is.

E törvény alkalmazásában:

> *6. elektronikus információs rendszer: az adatok, információk kezelését végző eszköz, eljárás, illetve ezek együttese, valamint az ezek működtetéséhez szükséges infrastruktúra;*
> *[2024. évi LXIX. törvény 4. § 6. pont]*

Ha a magyar szervezet kezében van az „eljárás” (konfiguráció) és az „adatok” kezelése, akkor a rendszer ezen rétegei felett rendelkezési joggal bír. Ez azt jelenti, hogy a rendszert fel kell venni az EIR nyilvántartásba saját rendszerként, és biztonsági osztályba kell sorolni, de a védelmi intézkedések megvalósítása megoszlik.

Ebben a hibrid modellben a biztonsági osztályba sorolás megtörténik (pl. Jelentős biztonsági osztály), és a 7/2024. (VI. 24.) MK rendelet szerinti kontrollokat két csoportra kell bontani a *rendszerbiztonsági tervben*.

A) A magyar szervezet által közvetlenül megvalósítandó kontrollok

Mivel a konfiguráció és a jogosultságkezelés a helyi szervezet kezében van, az ehhez kapcsolódó biztonsági követelményekért közvetlenül felelős. Ha például egy rossz konfiguráció miatt adatszivárgás történik, az a magyar ügyvezető felelőssége.

Ide tartozó követelmények a 7/2024. MK rendeletből:

- Hozzáférések kezelése, felhasználói fiókok létrehozása, törlése, jelszóházirend kikényszerítése. [2.2, 2.3, 2.5, 2.6, 8.22]
- Konfigurációkezelés, az ERP modulok beállításainak biztonsága, változáskezelés jóváhagyása. [6.7, 6.23, 6.26, 6.45]
- Naplózás elemzése, a magyar felhasználók tevékenységének monitorozása (ha van rá hozzáférés). [4.2, 4.13, 18.13]

Ha az infrastruktúra (szerverek, OS, hálózat, fizikai védelem) felett az anyavállalat rendelkezik a kiberbiztonsági a követelményeket a magyar szervezet nem tudja közvetlenül végrehajtani, ezért szerződéses kötelezettségként kell megkövetelnie a teljesülésüket.

Ide tartozó követelmények:

- Fizikai és környezeti biztonság, Szervertermek védelme; [7.1, 7.2, 7.3, 7.4, 7.5, 7.10, 7.12, 7.13, 7.14, 7.15, 7.18]
- Üzemeltetés biztonsága, hardver karbantartás, OS patch menedzsment; [11.1, 11.2, 11.3, 11.4, 6.25, 13.1, 13.2, 13.3, 13.4, 13.5]
- Mentések technológiai végrehajtása. [15.1, 15.2, 15.3, 15.5, 15.7, 15.9]

Részleges rendelkezési jog esetén az 1/2025. (I. 31.) SZTFH rendelet alapján végzett audit során az auditor a következőképpen jár el:

1. Elfogadja a rendszert részlegesen rendelkezésben lévőként, mivel a magyar fél konfigurálja.
2. A helyi kontrollokat élesben vizsgálja, pl bizonyítékot kér arról, hogy a jelszóházirend tényleg be van-e állítva, a kilépett dolgozók jogosultsága vissza van-e vonva.
3. A központi kontrollokat dokumentum alapon vizsgálja, bekéri az érvényes szerződést, az SLA riportokat és a biztonsági garanciákat igazoló dokumentumokat.

Kockázatos pont, ha a magyar szervezetnek van konfigurációs joga, de elmulasztja a biztonsági beállításokat (pl. gyenge jelszót engedélyez, vagy nem tartja be a legkisebb jogosultság elvét), az auditon nem megfelelőséget fog kapni. Ilyenkor a magyar cég nem hivatkozhat arra, hogy „ez az anyavállalat rendszere”.

3.3 Biztonsági osztályba sorolás kötelezettsége

A biztonsági osztályba sorolás kötelezettsége a jogszabály szövege szerint szűkebb körű, mint a nyilvántartási kötelezettség. A törvény szerint a szervezet csak a rendelkezésében lévő rendszereket köteles osztályba sorolni.

> *E törvény alkalmazásában a szervezet elektronikus információs rendszerének kell tekinteni a szervezet rendelkezésében lévő elektronikus információs rendszert.*

> *A szervezet vezetője […] gondoskodik az 1. pont a) alpontja szerinti elektronikus információs rendszereknek [a szervezet rendelkezésében lévő rendszerek] az informatikáért felelős miniszter rendeletében meghatározottak szerint biztonsági osztályba sorolja […]*
> *[2024. évi LXIX. törvény 6. § (3) bekezdés 4. pont]*

Ha az ERP rendszer felett a magyar szervezetnek nincs rendelkezési joga (nem ő az üzemeltető, nem ő dönt a konfigurációról), akkor a rendszert magát nem kell és nem is tudja biztonsági osztályba sorolni a magyar jogszabályok szerint.

A szervezetnek a szolgáltatóval (anyavállalattal) szemben érvényesítenie kell a biztonsági követelményeket, hiányzó vagy részleges rendelkezési jog esetén.

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.*
> *16.49.2. Meghatározza és dokumentálja a szervezeti felügyelet és a szervezet felhasználóinak feladatait és kötelezettségeit a külső EIR-ek szolgáltatásával kapcsolatban.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 16.49. pont (A, J, M - kötelező)]*

3.4 Kivonható-e az EIR a lokális audit hatálya alól?

Ha szervezetnek nincs rendelkezési joga egy adott rendszer felett akkor igen. Ha részleges a rendelkezési jog, például az anyavállalat üzemelteti az rendszert, de a felhasználókezelés és konfiguráció az szervezet feladata, akkor maga a központi infrastruktúra (szerverek, adatbázisok) fizikailag és logikailag kivonható a közvetlen technikai vizsgálat alól, de a rendszer használata és a hozzá kapcsolódó kockázatkezelés nem.

> *Az 1/2025. (I. 31.) SZTFH rendelet szerint az audit tárgya a szervezet rendelkezésében lévő rendszerek osztályba sorolása és a védelmi intézkedések alkalmazása.*
> *A kiberbiztonsági audit során az auditor ellenőrzi […] a szervezet valamennyi elektronikus információs rendszerének biztonsági osztályba sorolása, valamint […] a szervezet auditor által kijelölt elektronikus információs rendszerei biztonsági osztályának megfelelő […] védelmi intézkedések alkalmazását […]*
> *[1/2025. (I. 31.) SZTFH rendelet 1. § (2) bekezdés]*

Mivel az ERP nincs a szervezet rendelkezésében (így nincs besorolva), az auditor nem fogja a szerveroldali hardeninget vagy a patch menedzsmentet közvetlenül vizsgálni az anyavállalatnál. Azonban az audit kiterjed a következőkre, amelyek érintik az ERP használatát:

- Külső rendszerek használata, az auditor vizsgálni fogja, hogy a szervezet hogyan győződött meg arról, hogy az anyavállalat által nyújtott ERP biztonságos. (Beszállítói kockázatelemzés).

- Kliens oldali védelem, azok a munkaállomások, amelyeken az ERP klienst futtatják, a magyar szervezet rendelkezésében vannak, így azok auditkötelesek.
- Jogosultságkezelés, hogyan igénylik és vonják vissza a magyar munkavállalók ERP hozzáférését.

4. FORRÁSOK

- Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény
- 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