Mi a teendő, ha egy cég tevékenységének csak egy része tartozik a Kiberbiztonsági tv. hatálya alá?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/22

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.26	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Ez a dokumentum azt a gyakori üzleti és megfelelőségi kérdést vizsgálja, hogy mi a teendő abban az esetben, ha egy vállalat tevékenységének csupán egy része (például a szoftverfejlesztés) esik a Kiberbiztonsági törvény hatálya alá, míg más üzletágai (például a könyvelés) nem.

Legfontosabb stratégiai megállapítások:

- A szervezeti hatály teljes körű. A Kiberbiztonsági tv. és a 7/2024. (VI. 24.) MK rendelet előírásait a teljes vállalatnál, a jogi személy egészénél alkalmazni kell.
- Nincs részleges megfelelés, a jogszabályok nem ismerik a "részleges hatály" vagy a "divíziós szintű kötelezettség" fogalmát a kötelezetti minőség megállapítása során.
- Minden informatikai rendszert biztonsági osztályba kell sorolni. Az előírások vonatkoznak azon elektronikus információs rendszerekre (EIR) is, amelyek nem a kockázatos vagy kiemelten kockázatos ágazatba tartozó tevékenységeket szolgálják ki.
- Kockázatarányos védelem elve alapján lehetőség van költségoptimalizálásra. Az alacsonyabb kockázatú, megfelelően szegmentált üzletágak (pl. könyvelés) rendszerei az „Alap” biztonsági osztályba sorolhatók, így rájuk enyhébb védelmi intézkedések vonatkozhatnak.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy cégben adott két teljesen elkülönült szolgáltatás/feladatkör. Például a cég szoftverfejlesztést, végez, amely üzemeltetéssel és támogatással párosul valamint könyvelési szolgáltatást nyújt. Az egyik tevékenység a Kiberbiztonsági tv. hatálya alá tartozik, a másik nem,

Kérdések:

- Ilyenkor a teljes cégnél kell a Kiberbiztonsági tv. és 7/2024 (VI,24) MK rendelet előírásait alkalmazni vagy csak a kötelezett részen?
- A 7/2024 (VI,24) MK rendelet elírásait alkalmazni kell azon EIR-ekre is, amelyek nem relevánsak a kockázatos vagy kiemelten kockázatos ágazatba tartozó tevékenységek kapcsán?

3. VÁLASZ

3.1 A vizsgált esetben a teljes cégnél kell a Kiberbiztonsági tv. és 7/2024 (VI. 24.) MK rendelet előírásait alkalmazni vagy csak aNIS2 kötelezett részlegeknél?

A jogszabályok előírásait a teljes cégnél, azaz a jogi személy egészénél alkalmazni kell. A kiberbiztonsági szabályozás alanya maga a "szervezet", mint önálló, egységes jogi entitás (pl. Kft., Zrt.), nem pedig annak egy-egy üzletága vagy tevékenysége. Ha egy cég a

szoftverfejlesztési tevékenysége és mérete alapján a törvény hatálya alá kerül, akkor maga a jogi személy válik kötelezetté.

A Kiberbiztonsági tv.. alanyi és tárgyi hatályát a törvény 1. §-a rögzíti, amely egyértelművé teszi a jogalkotói szándékot: a kötelezettségek alanya a jogi személyiséggel rendelkező "szervezet" mint egységes egész, és nem az egyes elszigetelt tevékenységek, divíziók vagy üzletágak.

A hazai polgári jogi dogmatika és a Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.) alapvetései alapján a jogi személyiség egységes és oszthatatlan. Egy gazdálkodó szervezet (például egy korlátolt felelősségű társaság vagy egy zártkörűen működő részvénytársaság) egyetlen cégjegyzékszámmal, egyetlen adószámmal és egyetlen egységes jogi felelősséggel rendelkezik. A Kiberbiztonsági tv. fogalomkészlete is ezt az egységet tükrözi:

> *„szervezet: az állami szerv vagy állami szervezet, a Polgári Törvénykönyvről szóló törvény szerinti jogi személy, jogi személyiség nélküli szervezet...” [2024. évi LXIX. törvény 4. § 91. pont]*

Ebből a jogszabályi definícióból és a dogmatikai alapvetésből logikusan következik, hogy amennyiben egy szervezet bármely, a cégjegyzékben bejegyzett és ténylegesen gyakorolt tevékenysége alapján a Kiberbiztonsági tv 2. vagy 3. mellékletében felsorolt ágazatok valamelyikébe tartozik (például szoftverfejlesztés, digitális infrastruktúra üzemeltetés), és eléri a jogszabályban meghatározott méretküszöböt (azaz legalább középvállalkozásnak minősül, vagy a pénzügyi mutatói meghaladják a határértékeket), úgy maga a jogi személy válik a törvény kötelezettjévé.

A jogszabály nem ismeri a "részleges hatály", a "tevékenység-specifikus alanyi hatály" vagy a "divíziós szintű kötelezettség" fogalmát a kötelezetti minőség megállapítása során. Amikor a vizsgált vállalat szoftverfejlesztési és üzemeltetési tevékenysége miatt eléri a jogszabályi küszöböt, a vállalat egésze, mint egyetlen jogi entitás kerül be a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH) által vezetett közhiteles hatósági nyilvántartásba.

A 7/2024. (VI. 24.) MK rendelet is egyértelművé teszi, hogy az abban meghatározott szervezeti szintű (adminisztratív, logikai és fizikai) védelmi intézkedések a szervezet egészére és annak minden elektronikus információs rendszerére (EIR) irányadók. Ennek értelmében a vállalati szintű szabályzatoknak, a fizikai védelemnek vagy a biztonságtudatossági képzéseknek a könyvelési tevékenységet végző munkatársakra is ki kell terjedniük.

3.2 A 7/2024 (VI. 24.) MK rendelet előírásait alkalmazni kell azon EIR-ekre is, amelyek nem relevánsak a kockázatos vagy kiemelten kockázatos ágazatba tartozó tevékenységek kapcsán?

A 7/2024. (VI. 24.) MK rendelet előírásait alkalmazni kell a nem kockázatos vagy kiemelten kockázatos ágazatba tartozó tevékenységet kiszolgáló (például kizárólag a könyvelési üzletágat támogató) elektronikus információs rendszerekre is. A jogalkotó előírja, hogy a szervezet rendelkezésére álló valamennyi elektronikus információs rendszert biztonsági osztályba kell sorolni, és az adott osztálynak megfelelő védelmi követelményeket kell rajtuk érvényesíteni.

> *„A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) 1. § (1) bekezdése szerinti szervezet (a továbbiakban: szervezet) a rendelkezésében lévő, a Kiberbiztonsági tv. hatálya alá tartozó elektronikus információs rendszerét az 1. mellékletben felsorolt szempontok szerint sorolja biztonsági osztályba.” [7/2024. (VI. 24.) MK rendelet 1. § (2) bekezdés]*

A kiberbiztonsági auditot szabályozó 1/2025. (I. 31.) SZTFH rendelet kifejezetten előírja az auditor számára, hogy a szervezet valamennyi elektronikus információs rendszerének biztonsági osztályba sorolását ellenőriznie kell.

> *„A kiberbiztonsági audit során az auditor ellenőrzi [...] szervezet (a továbbiakban együtt: szervezet) valamennyi elektronikus információs rendszerének biztonsági osztályba sorolása, valamint” [1/2025. (I. 31.) SZTFH rendelet 1. § (2) bekezdés a) pontja]*
> *„Az auditor az 1. § (2) bekezdés a) pontja szerinti vizsgálat során ellenőrzi a 3. § (3) bekezdése szerint átadott, a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását tartalmazó nyilvántartásban foglalt valamennyi elektronikus információs rendszer biztonsági osztályba sorolásának megfelelőségét.” ” [1/2025. (I. 31.) SZTFH rendelet 5. melléklet) 2.1.1. pontja:]*

Ugyanakkor a kockázatarányos védelem elve érvényesül. Ha a könyvelési EIR egy megfelelően szegmentált hálózaton fut, és az üzletmenet szempontjából alacsonyabb kockázatot jelent, akkor vélhetően az "Alap" biztonsági osztályba fog kerülni, még akkor is, ha a szervezet NIS2 hatály alá tartozó tevékenysége „Jelentős” vagy „Magas” biztonsági osztályba tartozik. Ebben az esetben a könyvelési rendszereken csak az "Alap" szinthez rendelt, enyhébb védelmi intézkedéseket kell megvalósítani.

4. FELHASZNÁLT FORRÁSOK

- 2013. évi V. törvény a Polgári Törvénykönyvről szóló (Ptk.)
- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről