Mikor kell alkalmazni a tanúsított IKT-termékeket és szolgáltatásokat?

VFP2 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/3

VERZIÓKÖVETÉS

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

1. ÖSSZEFOGLALÁS

Jelen dokumentum a tanúsított információs és kommunikációs technológiai (a továbbiakban: IKT) termékek[1], IKT-szolgáltatások[2] vagy IKT-folyamatok[3] kötelező alkalmazására vonatkozó előírásokat vizsgálja egy NIS2 kötelezett vállalkozás esetében. A legfontosabb tanulságok:

- A kiberbiztonsági tanúsítás rendszere alapvetően az önkéntességen alapul, maga a tanúsítási keretrendszer létrehozása automatikusan nem követeli meg a tanúsított termékek, szolgáltatások általánosan kötelező igénybevételét.
- Speciális uniós vagy nemzeti jogszabályok előírhatnak kötelező használatot.
- Az egyes kiberbiztonsági követelményeknek való megfelelőség igazolására az adott IKT-termék, -szolgáltatás tanúsítványa evidenciába csatolható, és alkalmas a szervezet kockázatkezelésének, kiberbiztonsági felkészültségének alátámasztására.
- A tanúsított IKT-megoldások alkalmazásának hiánya önmagában, további vizsgálat nélkül nem utal magasabb kockázatosságra, és nem zárja ki azt sem, hogy a szervezetnél már bevezetett védelmi intézkedések a vonatkozó követelményeknek megfeleljenek.

2. PROBLÉMAFELVETÉS

A modern digitális környezetben a hálózati és információs rendszerek használata, az IKT-termékek és -szolgáltatások általános elterjedtsége a szervezetek működésének alapfeltételévé váltak, miközben a kiberfenyegetések volumene, komplexitása és hatása folyamatosan növekszik. Ezzel párhuzamosan az ellátási láncok globalizálódása és az összetett digitális ökoszisztémák megjelenése indokolttá tette a kiberbiztonsági tanúsítási rendszerek életre hívását, mint a bizalom és az összehasonlíthatóság eszközét. Az uniós és nemzeti szabályozás több szinten kezeli a kiberbiztonsági tanúsítást, ugyanakkor tisztázandó, hogy a tanúsítás, illetve a tanúsított termékek, szolgáltatások alkalmazása mikor jogszabályi kötelezettség, és mikor csupán kockázatkezelési és/vagy auditálhatósági eszköz.

[1] valamely hálózati vagy információs rendszer eleme vagy elemeinek csoportja - (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 12. pontja

[2] olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információ hálózati és információs rendszerek útján történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll - (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 13. pontja

[3] valamely IKT-termék vagy IKT-szolgáltatás tervezése, fejlesztése, rendelkezésre bocsátása illetve nyújtása vagy karbantartása céljából végzett tevékenységek összessége - (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 14. pontja

3. A KIBERBIZTONSÁGI TANÚSÍTÁS FOGALMA ÉS RENDSZERE

A kiberbiztonsági tanúsítás, illetve tanúsítvány célja, hogy egységes értékelési metódus alapján igazolja azt, hogy az adott IKT-termék, -szolgáltatás, -folyamat megfelel az adott tanúsítási rendszer biztonsági követelményeinek.

Az európai kiberbiztonsági tanúsítás szabályozási környezetének alapjait az ENISA-ról (a Kiberbiztonsági Ügynökségről), valamint az információs és kommunikációs technológia kiberbiztonsági tanúsításáról szóló (EU) 2019/881 rendelet (Cybersecurity Act) teremtette meg, egységes uniós keretet hozva létre az IKT-termékek, -szolgáltatások és -folyamatok kiberbiztonsági tanúsítására. A rendelet felhatalmazása alapján az ENISA végzi az európai tanúsítási rendszerek (sémák) kidolgozását és azok nyilvántartását. Az elfogadott európai tanúsítási rendszerek alapján kiadott tanúsítványokat szintén az ENISA teszi közzé a honlapján[4].

Az egyes IKT-megoldások tanúsítását az adott tanúsítási rendszer szabályai alapján az ún. megfelelőségértékelő szervezetek végzik, melyeket a nemzeti kiberbiztonsági tanúsítási hatóságok vesznek nyilvántartásba.[5]

A Cybersecurity Act ismeri továbbá a megfelelőségi önértékelés intézményét, mely során a megfelelőségértékelésre az IKT-termékek, az IKT-szolgáltatások vagy az IKT-folyamatok gyártójának vagy nyújtójának kizárólagos felelőssége mellett kerül sor. Az egyes tanúsítási rendszereknek egyértelműen szabályozni kell, hogy megengedett-e a rendszer keretei közt az önértékelés, azzal a korláttal, hogy arra a Cybersecurity Act megkötése szerint kizárólag az „alap” megbízhatósági szintnek megfelelő, alacsony kockázatot jelentő IKT-termékek, IKT-szolgáltatások, IKT-folyamatok vagy irányított biztonsági szolgáltatások esetében van lehetőség.[6]

Jelenleg egy elfogadott uniós tanúsítási sémát ismerünk, ez A közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC)[7], mely kizárólag az IKT-termékek, valamint védelmi profilok kiberbiztonságának értékelését és tanúsítását szolgálja.

A Cybersecurity Act szabályozási környezete lehetővé teszi továbbá, hogy amely területeken az unió nem rendelkezik elfogadott tanúsítási rendszerrel, ott a tagállamok nemzeti tanúsítási rendszert vezethetnek be és tarthatnak fenn mindaddig, amíg az arra vonatkozó uniós séma meg nem születik.

A magyar nemzeti kiberbiztonsági tanúsítási rendszer keretét a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) és annak végrehajtási rendeletei[8] adják.

---

[4] **https://certification.enisa.europa.eu/certificates**

[5] Magyarországon jelenleg kettő megfelelőségértékelő szervezet került nyilvántartásba vételre.

[6] Cybersecurity Act 53. cikk (1) bekezdés

[7] A Bizottság (EU) 2024/482 végrehajtási rendelete (2024. január 31.) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról

[8] Magyarország kiberbiztonságáról szóló 418/2024. (XII. 23.) Korm. rendelet, illetve az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló a 10/2023. (V. 15.) SZTFH rendelet

Magyarországon a nemzeti kiberbiztonsági tanúsító hatósági feladatokat a Szabályozott Tevékenységek Felügyeleti Hatósága (továbbiakban: SZTFH) látja el.

Az SZTFH – az ENISA-hoz hasonlóan – még csak egy esetben, az IoT-eszközök tanúsítására fogadott el nemzeti tanúsítási sémát [9].

4. IRÁNYMUTATÁS

4.1 Mikor kell alkalmazni a tanúsított IKT-termékeket és szolgáltatásokat?

Az európai kiberbiztonsági tanúsítás teljes rendszere alapvetően az önkéntességre épül, így a tanúsítási kötelezettség előírása és a tanúsított IKT-megoldások kötelező alkalmazásának elrendelése is csak kivételes esetben merülhet fel, mégpedig, ha azt az uniós vagy a magyar jogi szabályozás kifejezetten előírja.

A magyar szabályozás ezzel kapcsolatban a Kiberbiztonsági tv. 6. § (9) bekezdésében tartalmazza a speciális jogalkotói felhatalmazást:

„Az informatikáért felelős miniszter rendeletében – a honvédelmi célú elektronikus információs rendszerek tekintetében a honvédelmi miniszter rendeletében – meghatározott, 1. § (1) bekezdés a)–c) és f) pontja szerinti szervezetek, valamint az SZTFH elnökének rendeletében meghatározott, 1. § (1) bekezdés d) és e) pontja szerinti szervezetek kötelesek az európai vagy nemzeti kiberbiztonsági tanúsítási rendszer alapján tanúsított – az informatikáért felelős miniszter, a honvédelmi miniszter vagy az SZTFH elnöke rendeletében meghatározott – IKT-terméket, IKT-szolgáltatást vagy IKT-folyamatot használni.”

Mivel sem uniós szinten, sem - a fenti felhatalmazás alapján- nemzeti szinten nem született releváns jogszabály ebben a tárgykörben, ezért jelenleg egyetlen tanúsított IKT-termék, -szolgáltatás vagy -folyamat alkalmazása sem kötelező az érintett szervezetek részére.

4.2 Miért javasolt tanúsított IKT-terméket és szolgáltatást alkalmazni?

Habár a tanúsított IKT-termékek, -szolgáltatások, -folyamatok alkalmazása nem kötelező, mégis erősen ajánlott minden érintett szervezet részére, különösen az alábbi okokból:

- *Adminisztrációs ok:* A tanúsítvány független harmadik fél által kiadott bizonyíték, melynek birtokában az uniós szabályozás alapján vélelmezni kell, hogy az adott IKT-megoldás megfelel a tanúsítási rendszer által támasztott biztonsági követelményeknek.[10] A Kiberbiztonsági tv. által az érintett szervezetekkel szemben támasztott alapvető követelményeknek való megfelelés igazolására a tanúsított IKT-termék, -szolgáltatás, -folyamat alkalmazható[11]. Röviden a tanúsítvány önmagában alkalmas az adott követelménynek való megfelelőség igazolására, az esetleges értelmezési viták csökkentésére az auditor, a hatóság és a szervezet között.

[9] Az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszeréről szóló 10/2024. (VIII. 8.) SZTFH rendelet
[10] Cybersecurity Act 56. cikk (1) bekezdés
[11] Kiberbiztonsági tv. 6. § (8) bekezdés

- *Kiberbiztonsági okok:* A tanúsítvány az adott IKT-megoldás pontos leírását (verziószám/szolgáltatási modell), a tanúsítvány megbízhatósági szintjét[12] és érvényességi idejét[13], esetleges egyéb jellemzőket is tartalmaz, melyek – a tanúsítási rendszer egyedi követelményeinek ismeretében – hathatós segítséget nyújtanak a kockázatarányos intézkedések mérlegelésében, a fenyegetettségek felmérésében, az incidenskezelésben. Ezen folyamatokban szintén jelentős segítség továbbá, hogy a tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat gyártója vagy nyújtója köteles a tanúsított IKT-termékekkel, IKT-szolgáltatásokkal és IKT-folyamatokkal kapcsolatos egyes kiegészítő kiberbiztonsági információkat nyilvánosan elérhetővé tenni és naprakészen tartani.[14]
- *Átláthatóság, piaci szempontok:* A tanúsított IKT-megoldások használata növeli a bizalmat a felhasználók, partnerek és beszállítók körében, és összehasonlíthatóvá teszi a különböző megoldások kiberbiztonsági szintjét, ezáltal versenyelőnyt is jelenthet egyéb piaci szereplőkkel szemben.

Összefoglalva: A tanúsított IKT-megoldások alkalmazása stratégiai döntés, amelyet kockázatalapú megközelítéssel kell meghozni a NIS2 megfelelés érdekében.

A fentiekkel összhangban fontos azonban hangsúlyozni, hogy a tanúsított IKT-megoldások alkalmazása nem jelent automatikus jogszabályi mentességet, nem szünteti meg a folyamatos kockázatkezelés szükségességét és nem garantál abszolút biztonságot sem.

4.3 Hogyan ellenőrizhető a tanúsítás ténye?

Az európai kiberbiztonsági tanúsítási rendszerek alapján kiadott tanúsítványokat az ENISA a honlapján teszi közzé.[15] Emellett az európai kiberbiztonsági tanúsítási rendszerek a megfelelőségi jelölést is lehetővé tehetik. (Az EUCC hatálya alá tartozó IKT-termékek esetén a megfelelőségi címke és jelölés elhelyezése az EUCC szerint nem kötelező, a gyártó szabad belátásán múlik.[16])

A nemzeti tanúsítási rendszer alapján kiadott tanúsítványokkal kapcsolatban közzétételi kötelezettséget a hatósággal szemben nem támaszt a jogalkotó, azonban a 10/2023. (V. 15.) SZTFH rendelet a hatálya alá tartozó valamennyi IKT-megoldás kapcsán előírja az 1. melléklete szerinti jelölés kötelező alkalmazását. (Így a tanúsított IoT-eszközök esetében is kötelező a megfelelőségi jelölés alkalmazása, melyet *„jól láthatóan, egyértelműen és maradandóan kell elhelyezni.”*)

---

[12] *„A törvény rögzíti a nemzeti kiberbiztonsági tanúsítási rendszerek megbízhatósági szintjeit, azaz arra vonatkozóan szolgál biztosítékkal, hogy az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok teljesítik a vonatkozó biztonsági követelményeket, biztonsági funkciókat és olyan szintű értékelésen estek át, amely az adott szinteknek megfelelő súlyú kiberbiztonsági fenyegetések, támadások kockázatainak minimalizálására törekszik.”*- Kiberbiztonsági tv. 40. §-hoz fűzött indokolása

[13] Az EUCC alapján az IKT-termékre kiadott tanúsítvány maximum 5 évre érvényes. A 10/2024. (VIII. 8.) SZTFH rendelet szerint az IoT-eszközökre kiadott tanúsítvány érvényességi ideje a kiállítás napjától számított 365 nap.

[14] Cybersecurity Act 55. cikke

[15] Jelenleg 11 EUCC tanúsítvány érhető el a **https://certification.enisa.europa.eu/certificates** oldalon.

[16] A címke és jelölés formája az EUCC IX. mellékletében található.

A tanúsítvány megléte, pontos tartalma kapcsán mindig tájékozódjon hiteles forrásból, kétség esetén keresse az illetékes kiberbiztonsági tanúsítási hatóságot!

4.4 Mi az a megfelelőségi nyilatkozat?

Mind az uniós, mind a hazai szabályozás alapján az európai és nemzeti tanúsítási rendszer lehetővé teheti bizonyos korlátok között a megfelelőségi önértékelést. A megfelelőségi önértékelés abban tér el a tanúsítástól, hogy itt nem egy független harmadik személy végzi el az adott IKT-megoldás megfelelőségének értékelését, hanem maga az adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat gyártója vagy nyújtója. Ezen önvizsgálat eredményeként a gyártó ún. megfelelőségi nyilatkozatot állíthat ki, mellyel igazolja és egyben felelősséget vállal azért, hogy az IKT-termék, az IKT-szolgáltatás, az IKT-folyamat megfelel az adott tanúsítási rendszer által előírt követelményeknek.

Megfelelőségi önértékelésre csak az „alap” megbízhatósági szintnek megfelelő IKT-termékek, IKT-szolgáltatások, IKT-folyamatok esetében adhat lehetőséget a tanúsítási rendszer.[17]

Attól függően, hogy uniós vagy nemzeti tanúsítási rendszer hatálya alá tartozó megoldásról van-e szó a gyártó a kiállított uniós vagy nemzeti megfelelőségi nyilatkozatot köteles megküldeni az illetékes hatóság (ENISA; SZTFH) részére.

Amennyiben a megfelelőségi nyilatkozat kiállításra kerül és azt a hatóság nyilvántartásba veszi, úgy a gyártó jogosult a megfelelőségi címke és jelölés tanúsítási rendszer szerinti elhelyezésére is.

5. FORRÁSOK

- Az Európai Parlament és a Tanács 2019. április 17-i (EU) 2019/881 rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről
- A Bizottság (EU) 2024/482 végrehajtási rendelete (2024. január 31.) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról
- Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény
- Az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló 10/2023. (V. 15.) SZTFH rendelet
- Az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszeréről 10/2024. (VIII. 8.) SZTFH rendelet

[17] Mivel az EUCC hatálya alá tartozó IKT-termékek tanúsítható megbízhatósági szintje kizárólag „jelentős” vagy „magas” lehet, ezért a 6. cikk ki is zárja a megfelelőségi önértékelés lehetőségét. A 10/2024. (VIII. 8.) SZTFH rendelet az önértékelést az „alap” megbízhatósági szint esetében lehetővé teszi a hatálya alá tartozó IoT-eszközök esetén.