

Elfogadható-e, hogy az információbiztonsági architektúra leírás a rendszerbiztonsági terv részét képezi?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/50

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.23	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A 7/2024. (VI. 24.) MK rendelet az elektronikus információs rendszer (EIR) információbiztonsági architektúra leírását a jelentős és a magas biztonsági osztályban követeli meg, az alap osztályban nem. A leírás kötelező elemei:

- összegzi a bizalmasság, a sértetlenség és a rendelkezésre állás védelmét szolgáló követelményeket és a védelem megközelítését,
- bemutatja, hogyan illeszkedik a szervezet általános architektúrájába,
- rögzíti a külső szolgáltatásokkal kapcsolatos feltételezéseket és függőségeket.

A leírást a szervezeti architektúra változásakor felül kell vizsgálni, a tervezett változásokat pedig át kell vezetni a rendszerbiztonsági tervbe.

A fogalom a NIST SP 800-53 kontrollkatalógus PL-8 kontrolljának fordítása. A NIST szerint az architektúra leírás a védelem felépítését mutatja be, vagyis azt, hogy a védelmi intézkedések mely rendszerelemekhez és rétegekhez tartoznak, milyen külső interfészei vannak a rendszernek, azokon milyen információ halad át, és az interfészeket milyen mechanizmus védi.

Álláspontunk szerint elfogadható, hogy az architektúra leírás a rendszerbiztonsági terv részét képezze. A rendelet a leírás elkészítését követeli meg, önálló dokumentum kiadását nem. A NIST kifejezetten kimondja, hogy a rendszerbiztonsági tervnek nem kell egyetlen dokumentumnak lennie, a működési koncepcióról pedig azt, hogy az a tervbe foglalható. Az egybefoglalásnak feltételei vannak. A leírásnak a terven belül címében is azonosítható fejezetet kell kapnia, tartalmaznia kell mindhárom kötelező elemet, a terv frissítését kiváltó események közé be kell venni a szervezeti architektúra változását, és a védelmi intézkedések megvalósításánál a 13.6. pontnál erre a fejezetre kell hivatkozni.

Különálló dokumentumot akkor javasolunk, ha több EIR közös infrastruktúrán osztozik, ha a fejlesztés kiszervezett és a fejlesztőtől is architektúrát kell megkövetelni, vagy ha az architektúra gyakrabban és más gazdánál változik, mint a terv többi része. Az NKI rendszerbiztonsági terv sablonja mindkét megoldást támogatja, a Tervezés követelménycsoportot azonban nem tartalmazza, ezért a 13.6. pontot a szervezetnek kell a sablonba felvennie.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2¹-kötelezett szervezet (a továbbiakban mint „Szervezet”) jelentős biztonsági osztályba sorolt elektronikus információs rendszerének rendszerbiztonsági tervét készíti, és azzal szembesül, hogy a 7/2024. (VI. 24.) MK rendelet 2. mellékletének 13.6. pontja információbiztonsági architektúra leírást vár el tőle. A rendelet a fogalmat nem határozza meg, és nem mondja ki, hogy a leírásnak önálló dokumentumnak kell-e lennie. Az informatikai vezető

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)

a leírást a terv műszaki fejezetébe illesztené, az információbiztonsági felelős pedig külön dokumentumot készítené, mert attól tart, hogy az auditor azt fogja keresni.

Az állásfoglalás az alábbi kérdéseket vizsgálja:

- Mit jelent az információbiztonsági architektúra leírás, és mi az elvárt tartalma.
- Mely szabványokban lehet utánanézni annak, mire gondolt a jogalkotó.
- Képezheti-e a leírás a rendszerbiztonsági terv részét, és ha igen, milyen feltételekkel.

A szervezeti architektúra módszertana és a hálózattervezés műszaki kérdései nem tárgyai az állásfoglalásnak.

3. GYAKORLATI JAVASLATOK

3.1 Az architektúra leírás javasolt tartalma

Javasoljuk, hogy a leírás legalább a következőket tartalmazza.

- a) A védelmi célok és a megközelítés összegzése, a biztonsági osztályból és az adatosztályozásból levezetett követelmények, valamint a védelem vezérelvei (mélységi védelem, legkisebb jogosultság, zónákra bontás, alapértelmezett tiltás).
- b) A biztonsági zónák és rétegek, a zónák közötti határok, és annak bemutatása, hogy az egyes védelmi intézkedések (szűrés, hitelesítés, titkosítás, naplózás, mentés) mely helyekhez és rétegekhez tartoznak.
- c) A külső interfészek, minden kapcsolat más EIR-rel, külső hálózattal vagy szolgáltatással, az átadott információ típusa és az interfészt védő mechanizmus.
- d) Az illeszkedés a szervezeti architektúrába, a rendszer helye a szervezet rendszertérképén és a közösen használt szolgáltatásokból (címtár, naplógyűjtés, mentés, határvédelem) átvett védelmi intézkedések.
- e) A külső szolgáltatásokra vonatkozó feltételezések és függőségek, a felhő- és SaaS-szolgáltatások, a külső üzemeltetők és fejlesztők, a felelősségmegosztás, és az, hogy a Szervezet a szolgáltatótól milyen védelmi intézkedést vár el, és ezt mire alapozza.
- f) Az architektúrális döntések és kockázati mérlegelésük, a választott megoldások indoklása, az elfogadott eltérések és a helyettesítő intézkedések.
- g) A karbantartás szabályai, a verzió, a jóváhagyó, a felülvizsgálatot kiváltó események és a változások átvezetésének módja.

3.2 Hogyan illeszthető a leírás a rendszerbiztonsági tervbe

Két megoldás egyaránt elfogadható. Az első szerint a leírás a terv önálló fejezete. Az NKI sablonjában ennek természetes helye a műszaki megoldásokat bemutató 5. fejezet után egy új, „Információbiztonsági architektúra leírás” című fejezet, amely a topológiára már leírt tartalomra hivatkozik, és azt a fenti elemekkel egészíti ki. A második szerint a leírás külön dokumentum, amelyet a terv a kapcsolódó dokumentumok között sorol fel, és amelyre a 13.6. pontnál hivatkozik.

Nem elfogadható viszont, ha a Szervezet a hálózati topológia ábráját tekinti architektúra leírásnak, és az sem, ha a három kötelező elem a tervben szétszórva, cím és azonosíthatóság nélkül szerepel, mert az auditor a 13.6. pont teljesülését keresi, és ennek bizonyítékát meg kell tudni mutatni neki.

A sablon 8. fejezete a védelmi intézkedések megvalósítását tíz követelménycsoportra bontva tartalmazza, a Tervezés csoportot nem, ezért a 13.2. és a 13.6. pontot a Szervezetnek magának kell felvennie, a 13.6. sorban a leírás fejezetére utalva.

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, kiberbiztonsági felügyeletét a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) látja el,² és az érintett EIR jelentős biztonsági osztályba tartozik. A válasz a magas osztályú rendszerekre és a többi szervezettípusra is irányadó, az 1. § (1) bekezdés a)-c) és f) pontja alá tartozó szervezetek eltéréseit a 4.5. pont foglalja össze.

A Szervezet vezetője határozza meg az EIR-ek kockázatokkal arányos védelmi intézkedéseit,³ és dönt a rendszer használatbavételéről vagy használatának folytatásáról.⁴ A rendelet 1. melléklete szerint a szervezet az alkalmazandó biztonsági követelményeket a rendszerbiztonsági tervben dokumentálja, amelyet a szervezet vezetője vagy az információbiztonsági felelős hagy jóvá,⁵ a használatbavételről pedig a vezető többek között a rendszerbiztonsági terv alapján dönt.⁶ A részletes követelményeket a rendelet 2. mellékletének 13. (Tervezés) követelménycsoportja tartalmazza, amely a NIST SP 800-53 ötödik kiadásának PL (Planning) kontrollcsaládját követi.⁷

4.2 Az információbiztonsági architektúra leírás fogalma és elvárt tartalma

4.2.1 A rendelet a jelentős és a magas osztályban követeli meg

A rendelet a leírást a 13.6. pontban írja elő, a követelmény a jelentős és a magas osztályban kötelező.

13.6. A szervezet:

13.6.1. Elkészíti az EIR információbiztonsági architektúra leírását.

13.6.1.1. Összegzi az EIR bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló követelményeket és megközelítést.

² 2024. évi LXIX. tv. 23. § (1) bekezdés b) pont

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

⁴ 2024. évi LXIX. tv. 6. § (3) bekezdés 12. pont

⁵ 7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.3. pont

⁶ 7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.6. pont

⁷ NBSZ NKI, Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, Előkészületek, 1.0 verzió (2024. augusztus). Az útmutató szerint a rendelet védelmi intézkedései a NIST SP 800-53 ötödik kiadására épülnek.

13.6.1.2. Megfogalmazza, hogy az információbiztonsági architektúra hogyan illeszkedik a szervezet általános architektúrájába, és hogyan támogatja azt.

13.6.1.3. Leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket.

13.6.2. Az általános architektúrájában bekövetkezett változtatásokra reagálva felülvizsgálja és frissíti az információbiztonsági architektúra leírást.

13.6.3. Biztosítja, hogy az információbiztonsági architektúra leírásban tervezett változtatás tükröződjön a rendszerbiztonsági tervben, a működési koncepcióban és a beszerzésekben. [7/2024. (VI. 24.) MK rendelet 2. melléklet 13.6. pont] (J, M)

A mélységi védelem elvén alapuló tervezés és a beszállítói diverzifikáció opcionális kiegészítés,⁸ ahogyan az EIR információbiztonsági szempontú működtetését leíró működési koncepció is.⁹ Az alap osztályban két rokon követelmény él. A szervezet minden EIR-nél dokumentumban rögzíti a rendszer helyét a szervezeti architektúrában, ha a szervezet ilyennel rendelkezik,¹⁰ és minden osztályban kialakítja és fenntartja a szervezeti szintű architektúrát.¹¹

4.2.2 A fogalom a NIST katalógus PL-8 kontrolljából ered

A 13.6. pont a NIST SP 800-53 Rev. 5 katalógus PL-8 (Security and Privacy Architectures) kontrolljának fordítása. A három tartalmi elem a PL-8 a) pont 1., 3. és 4. alpontja, a személyes adatokra vonatkozó 2. alpontot a magyar szöveg nem vette át, a 13.7. és a 13.8. pont a PL-8 (1) és (2) kontrollbővítése.

A NIST magyarázata szerint a rendszerszintű biztonsági architektúra a szervezeti szintű architektúrával összhangban készül. Tartalmazza az architekturális leírást, a biztonsági funkciók és védelmi intézkedések hozzárendelését a rendszer elemeihez, a külső interfészekre vonatkozó biztonsági információkat, az azokon átadott információkat és az egyes interfészekhez tartozó védelmi mechanizmusokat.¹² Az architektúra leírás tehát nem a rendszer műszaki dokumentációja, hanem a védelem felépítésének bemutatása. Azt válaszolja meg, hogy a szervezet a követelményeket milyen elvek mentén, milyen rétegekben és milyen elemekkel teljesíti, hol vannak a rendszer határai, és mit bíz külső félre.

4.2.3 Elhatárolások

⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.7. pont (O) és 13.8. pont (O)

⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.5. pont (O)

¹⁰ 7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.1.2.7. pont

¹¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 1.7. pont (A, J, M). A pont a NIST PM-7 (Enterprise Architecture) kontroll fordítása, a magyar szövegben „szervezeti szervezetrendszer” szerepel.

¹² NIST SP 800-53 Rev. 5, PL-8 Security and Privacy Architectures, Discussion. „The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface.”

A rendszertopológia nem architektúra leírás. A topológia a rendszerelemeket és kapcsolataikat ábrázolja, az architektúra leírás erre épül, de azt mutatja be, hogy a védelem hogyan helyezkedik el ezen a szerkezeten.

A szervezeti architektúra nem az EIR architektúrája. A NIST szerint a szervezeti szintű architektúrát a PM-7, a rendszerszintűt a PL-8 kontroll írja le.¹³ A rendeletben az 1.7. pont a szervezeti, a 13.6. pont a rendszerszintű követelmény, a 13.6.1.2. pont pedig a kettő kapcsolatát kéri számon.

A fejlesztői architektúra nem a szervezet architektúra leírása. A magas osztályban a szervezet a fejlesztőtől is tervezési specifikációt és biztonsági architektúrát követel meg, amely illeszkedik a szervezet biztonsági architektúrájához.¹⁴ A fejlesztő architektúrája a szervezet saját leírását nem pótolja.

Az architektúra leírás végül nem azonos a rendszerbiztonsági tervvel. A terv a NIST szerint a követelményeket kapcsolja össze a védelmi intézkedésekkel, a megvalósítás részletes műszaki leírását azonban nem tartalmazza.¹⁵ A két tartalom egymásra épül, és ez egy dokumentumon belül is fenntartható.

4.3 Szabványok, amelyekben utána lehet nézni, mire gondolt a jogalkotó

4.3.1 A NIST kiadványok

Az első forrás maga a NIST SP 800-53 Rev. 5 katalógus, azon belül a PL-8, a PL-2, a PL-7, a PM-7 és az SA-17 kontroll magyarázata. A rendelet 13.2. pontja a PL-2, a 13.5. pontja a PL-7, a 13.6. pontja a PL-8 fordítása. A NIST SP 800-53A Rev. 5 az értékelési eljárásokat tartalmazza. A PL-8 értékelésénél vizsgálendő bizonyítékok között a szervezeti architektúra dokumentációja, az információbiztonsági architektúra dokumentációja és a rendszerbiztonsági terv egyaránt szerepel.¹⁶ Az értékelő tehát az architektúrát a rendszerbiztonsági tervben is keresheti.

A rendszerbiztonsági terv szerkezetére a NIST SP 800-18 az irányadó útmutató, amelynek második kiadása 2026 júniusában jelent meg.¹⁷ Az útmutató a terv elemei között a rendszerarchitektúra fő jellemzőinek összefoglalását, a külső szolgáltatók bemutatását, a működési környezet ábráit és a hálózati architektúra rajzait sorolja fel. A terv a NIST felfogásában eleve tartalmaz architekturális információt, az architektúra leírás ennek részletezése. A NIST SP 800-37 Rev. 2 kockázatmenedzsment keretrendszer az előkészítő lépésben külön feladatként nevezi meg a rendszer elhelyezését a szervezeti architektúrában, a

¹³ NIST SP 800-53 Rev. 5, PM-7 Enterprise Architecture, Discussion. „For PM-7, security and privacy architectures are developed at a system-of-systems level, representing all organizational systems. For PL-8, the security and privacy architectures are developed at a level that represents an individual system.”

¹⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 16.87. pont (M). A NIST SA-17 kontroll magyarázata szerint az SA-17 a külső fejlesztőnek, a PL-8 a szervezetnek szól, a kettő egymást kiegészíti.

¹⁵ NIST SP 800-53 Rev. 5, PL-2 System Security and Privacy Plans, Discussion. „The plans describe how the controls and control enhancements meet the security and privacy requirements but do not provide detailed, technical descriptions of the design or implementation of the controls and control enhancements.”

¹⁶ NIST SP 800-53A Rev. 5, PL-08 Examine, vizsgálendő objektumok, többek között „enterprise architecture documentation”, „information security and privacy architecture documentation”, „system security plan”.

¹⁷ NIST SP 800-18 Rev. 2, Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems, 2026. június, doi.org/10.6028/NIST.SP.800-18r2. A terv elemeit az útmutató 1. táblázata sorolja fel.

kiválasztási lépésben pedig a tervezett védelmi intézkedések dokumentálását a rendszerbiztonsági tervben,¹⁸ a NIST SP 800-160 Vol. 1 pedig az architektúra meghatározását a fejlesztési életciklus mérnöki folyamataként írja le.¹⁹

4.3.2 Az ISO szabványok

Az „architektúra leírás” kifejezés jelentését az ISO/IEC/IEEE 42010 (2022) szabvány rögzíti. A szabvány különbséget tesz a rendszer architektúrája és annak leírása között, a leírás az a munkatermék, amely az architektúrát az érintettek szempontjai szerinti nézetekben mutatja be.²⁰ A rendelet is a leírás elkészítését teszi kötelezővé, a leírás pedig bármely dokumentumban elhelyezhető munkatermék.

Az ISO/IEC 27001 (2022) szabvány A mellékletének 8.27. kontrollja a biztonságos rendszerarchitektúra és a mérnöki elvek kialakítását, dokumentálását, fenntartását és alkalmazását írja elő minden rendszerfejlesztési tevékenységre. Az ISO/IEC 27002 (2022) útmutatása szerint a biztonságot az architektúra valamennyi rétegében (üzleti, adat-, alkalmazás- és technológiai réteg) meg kell tervezni, az elveket pedig rendszeresen felül kell vizsgálni.²¹ A szabvány rendszerbiztonsági tervet nem ismer, a legközelebbi megfelelője az alkalmazhatósági nyilatkozat és a kockázatkezelési terv, a dokumentált információ formáját pedig a 7.5. pont a szervezetre bízta. Az ISO-alapú irányítási rendszert működtető szervezetnek a 13.6. pont elemeit ettől függetlenül be kell mutatnia. A módszertant a SABSA keretrendszer és a TOGAF biztonsági kiterjesztése dolgozza ki, ezek segítenek abban, hogy a leírás ne ábragyűjtemény, hanem rétegenként indokolt védelmi szerkezet legyen.

4.4 Képezheti-e az architektúra leírás a rendszerbiztonsági terv részét

4.4.1 A rendelet nem ír elő önálló dokumentumot

Ahol a jogalkotó önálló dokumentumot kíván, ott azt megnevezi. A 13.2.1. pont szerint a szervezet „rendszerbiztonsági tervet készít”, az 1. melléklet szerint a rendszerre vonatkozó adatokat „dokumentumban rögzíti”. A 13.6.1. pont ezzel szemben azt írja, hogy a szervezet „elkészíti az EIR információbiztonsági architektúra leírását”. A leírás tartalom, amelynek dokumentumformáját a rendelet nem határozza meg. Ugyanezt erősíti a 13.6.3. pont, amely nem a leírás kiadását, hanem azt követeli meg, hogy a leírásban tervezett változtatás a rendszerbiztonsági tervben tükröződjön. Ez a követelmény akkor is teljesíthető, ha a leírás a terv egyik fejezete, ilyenkor a terv védelmi intézkedéseket bemutató fejezeteinek kell követniük az architektúra fejezetben tervezett változást.

¹⁸ NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations, Prepare lépés, P-16 (Enterprise Architecture) és P-17 (Requirements Allocation) feladat, Select lépés, S-4 (Documentation of Planned Control Implementations) feladat.

¹⁹ NIST SP 800-160 Vol. 1 Rev. 1, Engineering Trustworthy Secure Systems (2022), Architecture Definition folyamat.

²⁰ ISO/IEC/IEEE 42010 (2022), Software, systems and enterprise, Architecture description. Az architektúra leírás az érintettek (stakeholders) szempontjait (concerns) nézőpontok (viewpoints) szerinti nézetekben (views) bemutató munkatermék (tartalmi összefoglalás).

²¹ ISO/IEC 27001 (2022) A melléklet 8.27. kontroll (Secure system architecture and engineering principles), ISO/IEC 27002 (2022) 8.27. pont, valamint ISO/IEC 27001 (2022) 6.1.3. d) pont (alkalmazhatósági nyilatkozat) és 7.5. pont (dokumentált információ). A szövegben tartalmi összefoglalás szerepel, nem szó szerinti idézet.

A rendszerbiztonsági terv kötelező tartalma ugyanerre az eredményre vezet.

13.2. A szervezet:

13.2.1. Az EIR-hez rendszerbiztonsági tervet készít, amely:

13.2.1.1. Összhangban áll a szervezeti felépítéssel.

13.2.1.2. Meghatározza az EIR-t alkotó rendszerelemeket.

[...]

13.2.1.8. Meghatározza az EIR működési környezetét és más EIR-ekkel vagy rendszerelemekkel való kapcsolatait vagy azoktól való függőségeit.

[...]

13.2.1.11. Meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket, intézkedésbővíítéseket és azok indoklását, végrehajtja a jogszabály szerinti biztonsági feladatokat. [7/2024. (VI.

24.) MK rendelet 2. melléklet 13.2. pont] (A, J, M)

A 13.6. pont három eleme ezekhez kapcsolódik, azokat biztonsági szempontból rendezi és értelmezi. A két tartalom átfed, és a rendelet ezt az átfedést nem tiltja, hanem az összhang követelményével kezeli. A NIST eredeti szövegében a terv kötelező eleme az architektúrális és tervezési döntések kockázati mérlegelése is, a magyar szövegből ez az elem kimaradt, a 13.2.1.12. és a 13.2.1.13. alpont azonos tartalommal szerepel. A NIST felfogásában tehát az architektúra a terv szerves része.

A NIST a kérdést kifejezetten megválaszolja. A PL-2 kontroll magyarázata szerint a rendszerbiztonsági tervnek nem kell egyetlen dokumentumnak lennie, a terv különböző, akár már meglévő dokumentumok gyűjteménye is lehet.²² A működési koncepcióról, amely a PL családban az architektúra leírás párja, a NIST kimondja, hogy az a rendszerbiztonsági tervbe vagy más életciklus-dokumentumba foglalható.²³ Ha a dokumentumhatár az egyik irányban átjárható, akkor a másik irányban is az, a terv magába foglalhatja azt a tartalmat, amelyet a katalógus máshol önálló kontrollként nevez meg.

Az auditor a védelmi intézkedések megfelelőségét ellenőrzi,²⁴ vagyis azt, hogy a 13.6. pont szerinti tartalom létezik, teljes, jóváhagyott és karbantartott, a dokumentum címe és a fejezetek elosztása nem megfelelőségi kérdés. Az NKI 2025 márciusában közzétett sablonjai is ezt tükrözik. A sablon 5. fejezete a rendszer határait, topológiáját és kapcsolatait kéri bemutatni, a 7.2. pontja a kapcsolódó dokumentumokat sorolja fel, és több helyen megengedi, hogy a terv más nyilvántartásra hivatkozzon.²⁵

²² NIST SP 800-53 Rev. 5, PL-2, Discussion. „Security and privacy plans need not be single documents. The plans can be a collection of various documents, including documents that already exist.”

²³ NIST SP 800-53 Rev. 5, PL-7 Concept of Operations, Discussion. „The CONOPS may be included in the security or privacy plans for the system or in other system development life cycle documents.”

²⁴ 2024. évi LXIX. tv. 21. § (1) bekezdés

²⁵ NBSZ NKI, A 7/2024. MK rendelet alapján aktualizált rendszerbiztonsági terv sablonok (2025. március 19.), Jelentős biztonsági osztály, V.1.0. Az 5.2.2. és az 5.2.3. pont megengedi a rendszerelemek nyilvántartására hivatkozást. A 8. fejezet tíz követelménycsoport védelmi intézkedéseit tartalmazza, a Tervezés csoport egyik sablonban sem szerepel.

Mindezek alapján álláspontunk szerint elfogadható, hogy az információbiztonsági architektúra leírás a rendszerbiztonsági terv részét képezze. A rendelet ezt nem zárja ki, a forrásként szolgáló NIST katalógus kifejezetten támogatja, az NKI sablon szerkezete pedig lehetővé teszi.

4.4.2 Az egybefoglalás feltételei

Az egybefoglalás akkor felel meg a rendeletnek, ha a terv a 13.6. pont valamennyi követelményét azonosíthatóan teljesíti. Ebből hat feltétel következik.

- A leírás a tervben önálló, a 13.6. pontra utaló című fejezet, amelyre a védelmi intézkedések megvalósítását bemutató rész a 13.6. sornál hivatkozik.
- A fejezet mindhárom tartalmi elemet tartalmazza. A topológia és a kapcsolatok leírására hivatkozhat, de az elemzést nem helyettesítheti velük.
- A terv frissítését kiváltó események között a szervezeti architektúra változása is szerepel. A 13.2.4. pont az EIR-ben és annak üzemeltetési környezetében történt változásokat nevezi meg, a 13.6.2. pont ennél tágabb.
- A jóváhagyás a tervre vonatkozó szabály szerint történik, a terv felülvizsgálatakor pedig az architektúra fejezetet is felül kell vizsgálni.
- A terv megismertetésének és védelmének szabályai az architektúra fejezetre is kiterjednek. Az architektúra leírás a terv legérzékenyebb része, mert a védelem felépítését mutatja meg, ezért a terjesztési kört ehhez kell igazítani.
- A változáskezelési eljárásrend rögzíti, hogy az architektúra tervezett változását a terv többi fejezetében és a beszerzésekben át kell vezetni, mert a 13.6.3. pont teljesülése egy dokumentumon belül sem automatikus.

4.4.3 Mikor célszerű mégis különválasztani

Külön dokumentumot javasolunk, ha több EIR osztozik ugyanazon az infrastruktúrán, mert ilyenkor a közös architektúra leírása egyszer készül el, és minden érintett terv hivatkozik rá. Ugyanez a helyzet, ha a fejlesztés kiszervezett, és a szervezet a fejlesztőtől is architektúrát követel meg, mert a kettő összevetése külön dokumentumban átláthatóbb. Különválasztás indokolt akkor is, ha az architektúra gazdája nem azonos a terv gazdájával, ha gyakrabban változik, mint a terv többi része, vagy ha a tervet szélesebb kör ismeri meg, mint amennyi az architektúra részleteire jogosult. A döntést a biztonságtervezési szabályzatban kell rögzíteni,²⁶ és úgy kell alkalmazni, hogy a 13.6. pont teljesülését egyetlen hivatkozással meg lehessen mutatni.

5. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS 2 irányelv)
- 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

²⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.1. pont (A, J, M)

- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- NBSZ NKI, Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, Előkészületek (1.0 verzió, 2024)
- NBSZ NKI, A 7/2024. MK rendelet alapján aktualizált rendszerbiztonsági terv sablonok, Alap, Jelentős és Magas osztály (V.1.0, 2025. március 19.)
- NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, valamint NIST SP 800-53A Rev. 5
- NIST SP 800-18 Rev. 2, Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems (2026. június)
- NIST SP 800-37 Rev. 2, Risk Management Framework, valamint NIST SP 800-160 Vol. 1 Rev. 1, Engineering Trustworthy Secure Systems
- ISO/IEC/IEEE 42010 (2022), Architecture description, valamint ISO/IEC 27001 (2022) és ISO/IEC 27002 (2022), 8.27. kontroll