

A folyamatos felügyeleti stratégia előírt tartalma és az ajánlott mérőszámok

VFP2 KiberVéd - NIS2 Audit felkészítés jogi
állásfoglalás 2026/42

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.16	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A folyamatos felügyeleti stratégia a 7/2024. (VI. 24.) MK rendelet szerint nem technikai monitoringterv, hanem a kockázatmenedzsment keretrendszer irányítási dokumentuma. Azt rögzíti, hogy a szervezet milyen mutatókkal, milyen gyakorisággal és milyen módszerrel győződik meg arról, hogy a védelmi intézkedések a változó környezetben is működnek, és a kockázatokkal arányosak maradnak. A rendelet két szinten írja elő, szervezeti szinten a 2. melléklet 1.23. pontjában és rendszerszinten a 2. melléklet 5.15. pontjában, mindkettő az alap biztonsági osztálytól kötelező. A kötelező tartalom hat, illetve hét elem, a mutatók, a gyakoriságok, a folyamatos értékelés és nyomon követés, az elemzés, a válaszlépések és a rendszeres jelentés.

A rendelet követelménykatalógusa a NIST SP 800-53 Rev. 5 kontrollkatalógus fordítása, a folyamatos felügyeletre vonatkozó pontok a PM-31 és a CA-7 kontrollnak felelnek meg. A jogszabályszoveg mögötti tartalmat a NIST SP 800-137 (a program lépései), a NIST SP 800-55 (a mérőszámok módszertana), valamint az ISO/IEC 27001 (2022) szabvány 9.1. pontja és az ISO/IEC 27004 szabvány adja meg.

Középvállalatnál a stratégia akkor működik, ha tíz és húsz közötti számú, a rendszerbiztonsági terv védelmi intézkedéseire kötött mutatóra épül. Ha a Szervezet monitoring és logelemző rendszert használ, a mutatók zöme automatikusan előállítható, a hangsúly a naplóforrás-lefedettség, a riasztáskezelési időköz, a sérülékenységek javítási átfutásán és a havi jelentésen van. Ha ilyen rendszer nincs, a stratégia továbbra is kötelező, a mutatókat kézi ellenőrzési naptárra, az eszközkonzolok jelentéseire és dokumentált átvizsgálásokra kell építeni. Jelentős vagy magas osztályú rendszerrel az automatizált naplóelemzés és a független értékelés kézi munkával nem váltható ki.

A szervezeti stratégia jóváhagyását a szervezet vezetőjének, a rendszerszintű stratégiáét az IBF-nek javasoljuk, a jelentéseket pedig legalább negyedévente a vezetés elé kell vinni. A dokumentum már az első kiberbiztonsági auditon is alapvető elvárás, annak hiánya vagy formális változata az auditor felé a keretrendszer működésének hiányát jelzi. A stratégia végrehajtásának gyakorlati bizonyítékai (a keletkezett mutatók és jelentések) pedig a további auditok kritikus feltételei lesznek.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy, a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja alá tartozó, középvállalat (a továbbiakban „Szervezet”) a rendszerbiztonsági tervek elkészítésekor szembesül azzal, hogy a 7/2024. (VI. 24.) MK rendelet több ponton folyamatos felügyeleti stratégiát vár el tőle, a fogalom tartalmát azonban néhány sorban írja le. Az állásfoglalás az alábbi kérdéseket vizsgálja:

- Mit takar a folyamatos felügyeleti stratégia a rendelet szerint, és mely biztonsági osztályokban kötelező?
- Milyen szabványok és ajánlások segítik a jogszabályszoveg értelmezését?
- Mi a stratégia ajánlott tartalma és mik az ajánlott mérőszámok egy középvállalatnál, ha a Szervezet monitoring és logelemző rendszert használ, és ha ilyen rendszere nincs?

Nem tárgya az állásfoglalásnak a naplózási követelmények részletes technikai tartalma, a biztonsági műveleti központ kiszervezése, valamint a honvédelmi célú rendszerek és a közigazgatási szervek sajátos szabályai.

3. GYAKORLATI JAVASLATOK

3.1 A stratégia javasolt felépítése

A Szervezet a stratégiát önálló, három és öt oldal közötti dokumentumként fogalmazza meg, amely a rendszerbiztonsági tervekre és a naplózási eljárásrendre hivatkozik. A javasolt fejezetek a következők.

- a) Cél, hatókör és szerepkörök, a felügyelt rendszerek biztonsági osztályuk szerint, az IBF, az informatikai vezető, a rendszergazdák és a vezetés feladatai, a külső szolgáltatók bevonása.
- b) A mutatók katalógusa, mutatónként a névvel, a mért védelmi intézkedéssel, az adatforrással, a számítás módjával, a célértékkel, a tűréshatárral és a felelőssel.
- c) Gyakoriságok, külön a mutatók gyűjtésére, a hatékonyság értékelésére, a sérülékenységi vizsgálatokra és a jelentésekre.
- d) Elemzés és válaszlépések, a tűréshatár átlépésekor követendő eljárás, az intézkedési tervbe való felvétel szabálya és az eskalációs útvonal.
- e) Jelentés és felülvizsgálat, a havi üzemeltetési és a negyedéves vezetői jelentés tartalma és címezettjei, a stratégia évenkénti és rendkívüli (új rendszer, incidens, auditmegállapítás, a besorolás változása) felülvizsgálata.

3.2 Ha a Szervezet monitoring és logelemző rendszert használ

Ilyenkor a stratégia a meglévő eszközre épít, és a mutatók többsége a rendszerből közvetlenül lekérdezhető. A javasolt elvek a következők.

- a) A naplóforrás-lefedettség a vezető mutató. A rendszerbiztonsági tervben szereplő rendszerelemek legalább 95 százaléka küldjön naplót a központi gyűjtőbe, és a 24 óránál régebben néma források száma nulla legyen.
- b) A riasztáskezelés idejét a Szervezet az észlelésig, a tudomásulvételig és a lezárásig eltelt idővel méri, súlyosság szerint bontva. Kritikus riasztásnál a tudomásulvétel egy órán, a lezárás egy munkanapon belül várható el. A hamis riasztások arányát negyedévente értékeli, mert a gondozatlan riasztási szabályok a felügyeletet formálissá teszik.
- c) A sérülékenységkezelés mutatói a szkennelési lefedettség, a kritikus és a magas súlyosságú sérülékenységek javítási átfutási ideje (javasolt célérték 14, illetve 30 nap) és a határidőn túli tételek száma.
- d) A hozzáférés-felügyelet mutatói a többtényezős hitelesítés lefedettsége a távoli és a privilegizált hozzáféréseknél, az inaktív fiókok száma és a jogosultság-felülvizsgálatok teljesítése. A havi jelentést a rendszer irányítópultja állítja elő, az IBF a negyedéves vezetői jelentésben trendekkel és javaslatokkal egészíti ki.

3.3 Ha a Szervezet nem használ monitoring és logelemző rendszert

A stratégia ilyenkor sem hagyható el, a különbség az adatforrásokban és a gyakoriságban van. A javasolt elvek a következők.

- a) A Szervezet ellenőrzési naptárt vezet, amely rendszerenként rögzíti, ki, milyen gyakorisággal és milyen ellenőrzőlista szerint nézi át a naplókat, az eszközkonzolokat és a mentési jelentéseket. Az átnézés ténye és eredménye jegyzőkönyvben marad fenn.
- b) A mutatók forrása a meglévő rendszerek beépített jelentése, például a címtár, a végpontvédelmi konzol, a frissítéskezelő, a tűzfal és a felhőszolgáltató biztonsági pontszáma, ezek exportja havonta egy közös táblázatba kerül.
- c) A sérülékenységi vizsgálatot a Szervezet negyedévente külső szolgáltatóval vagy ingyenes eszközzel végzi, a hozzáféréseket negyedévente címtárexport alapján, a mentéseket hetente, a helyreállítási tesztet félévente ellenőrzi és dokumentálja.

A kézi módszer csak alap osztályú rendszernél elegendő. Jelentős vagy magas osztályú rendszernél az automatizált naplóelemzés, a naplótárak összekapcsolása és a független értékelés kötelező.

3.4 A javasolt eljárás

A stratégia bevezetését az alábbi lépésekben javasoljuk.

- a) Leltár, a rendszerbiztonsági tervek, a besorolások és az adatforrások összegyűjtése, az automatikusan előállítható mutatók felmérése.
- b) Mutatóválasztás, tíz és húsz közötti mutató kiválasztása a NIST SP 800-55 módszertana szerint, célértékekkel és felelősökkel.
- c) Dokumentálás és jóváhagyás, a szervezeti és a rendszerszintű stratégia megírása és összehangolása a naplózási és a biztonságértékelési eljárásrenddel, vezetői, illetve IBF általi jóváhagyás.
- d) Próbaüzem és felülvizsgálat, három hónapos adatgyűjtés, a tűréshatárok kalibrálása, az első negyedéves jelentés elkészítése, majd a stratégia és a mutatók évenkénti, valamint audit vagy incidens utáni felülvizsgálata.

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 A vizsgálat kiindulópontjai

A Kiberbiztonsági tv. a védelmet a rendszer teljes életciklusára, zárt, teljes körű, folytonos és a kockázatokkal arányos módon követeli meg, ami önmagában feltételezi, hogy a szervezet a védelmi intézkedések működését időről időre ellenőrzi.¹ A kockázatmenedzsment keretrendszer a szervezet vezetőjének feladata, a keretrendszer fogalmában pedig a védelmi intézkedések nyomon követése és a fenyegetettségek folyamatos felderítése kifejezetten szerepel.² A vezető ezen belül köteles a védelmi intézkedések időszakos értékeléséről gondoskodni.

¹ 2024. évi LXIX. törvény 5. § (1) bekezdés és 4. § 99. pont

² 2024. évi LXIX. törvény 4. § 57. pont és 6. § (2) bekezdés

10. rendszeresen gondoskodik a védelmi intézkedések időszakszerű értékeléséről, ennek keretében legalább kockázatelemzések, ellenőrzések, független és a kiberbiztonsági hatóság által kiadott ajánlás szerinti belső kiberbiztonsági értékelés lefolytatása révén meggyőződik arról, hogy a jogszabályoknak és a kockázatoknak megfelelően meghatározott védelmi intézkedések megfelelően biztosítják-e a szervezet és elektronikus információs rendszerei biztonságát; [2024. évi LXIX. törvény 6. § (3) bekezdés 10. pont]

A törvény ehhez legalább kétévenkénti gyakoriságot rendel, ez azonban csak alsó határ, a rendelet folyamatos felügyeleti követelménye ennél sűrűbb, mutatókra épülő ellenőrzést vár el. A Szervezet az 1. § (1) bekezdés d) pontja szerinti szervezatként nem tartozik a 6. § (10) bekezdése szerinti könnyítés alá, ezért a teljes körű keretrendszer működtetnie kell, és a folyamatos felügyeletet is e keretben valósítja meg.³

4.2 Mit takar a fogalom a rendelet szerint

4.2.1 A keretrendszer szintje

A rendelet 1. melléklete a keretrendszer előkészítő lépései között írja elő a stratégia dokumentálását, itt még „biztonságfelügyeleti stratégia” néven, és már itt megnevezi a három kötelező tartalmi elemet, a gyakoriságot, a módszereket és az eszközöket.

1.1.1.1.3. a védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó biztonságfelügyeleti stratégiát, amely magába foglalja a védelmi intézkedésekhez kapcsolódó tevékenységek ellenőrzésének gyakoriságát, felügyeletének módszereit és eszközeit, [7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.1.1.3. pont]

A rendszerbiztonsági terv elkészítésekor a stratégiából rendszerszintű eljárásrend készül,⁴ a keretrendszer utolsó lépése pedig maga a folyamatos felügyelet.

1.1.7. a védelmi intézkedések folyamatos felügyeletével az elektronikus információs rendszer teljes életciklusa alatt gondoskodik arról, hogy a bekövetkezett szervezeti, technológiai és biztonsági környezetének változása esetén a védelmi intézkedések a kockázatokkal arányosak maradjanak. Ennek keretében [...]

1.1.7.2. a folyamatos felügyeleti stratégia alapján értékeli a rendszerben megvalósított védelmi intézkedéseket, azok állapotát rendszeresen jelenti a jogosult személyek felé, [7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.7. pont és 1.1.7.2. alpont]

³ 2024. évi LXIX. törvény 1. § (1) bekezdés d) pont, 6. § (4) bekezdés és 6. § (10) bekezdés

⁴ 7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.3. pont, utolsó mondat („A szervezet a folyamatos felügyeleti stratégiával összhangban kidolgozza a rendszerre vonatkozó védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó eljárásrendet;”)

A fogalom tehát a keretrendszer záró, felügyeleti lépése, a stratégia pedig azt írja le, milyen adatokból, milyen sűrűséggel és kinek a számára valósul meg.

4.2.2 A szervezeti szintű stratégia

A 2. melléklet programmenedzsment követelménycsoportja a stratégiát és a programot minden biztonsági osztályban előírja.

1.23. A szervezet folyamatos felügyeleti stratégiát fejleszt ki és folyamatos felügyeleti programot működtet, amely magában foglalja:

1.23.1. Az egész szervezet számára teljesítménymutatók meghatározását.

1.23.2. A felügyelet és a hatékonyság-értékelés gyakoriságának meghatározását.

1.23.3. A teljesítménymutatók folyamatos, a felügyeleti stratégia szerint történő figyelemmel kísérését.

1.23.4. A felügyelet és az elvégzett értékelések adatai közötti összefüggések és információk elemzését.

1.23.5. A védelmi intézkedések értékelések és felügyeleti információk eredményéből származtatott válaszlépések megtételét.

1.23.6. Az EIR biztonsági állapotáról rendszeres időközönként, a kijelölt személyeknek történő jelentést. [7/2024. (VI. 24.) MK rendelet 2. melléklet 1.23. pont] (A, J, M)

A követelmény hat kötelező tartalmi elemet ad, ezek a mutatók, a gyakoriságok, a folyamatos figyelés, az elemzés, a válaszlépések és a jelentés. A jogszabály a mutatók számát, típusát és a gyakoriságot nem határozza meg, ezeket a szervezet állapítja meg. Ez a rendelet és a NIST katalógus szerkesztési elve, a „szervezet által meghatározott” paraméter, amelyet a stratégiában kell kitölteni, különben a követelmény formálisan sem teljesül.

4.2.3 A rendszerszintű stratégia

5.15. A szervezet kidolgozza a rendszerszintű folyamatos felügyeleti stratégiát és megvalósítja a folyamatos felügyeletet a szervezeti szintű stratégiával összhangban, amely magában foglalja a következőket:

5.15.1. A rendszerszintű metrikák meghatározását.

[...]

5.15.7. az EIR biztonsági állapotáról rendszeres időközönként történő jelentés a kijelölt személyeknek. [7/2024. (VI. 24.) MK rendelet 2.

melléklet 5.15. pont, 5.15.1. és 5.15.7. alpont] (A, J, M)

A kihagyott 5.15.2. és 5.15.6. közötti alpontok a védelmi intézkedések rendszeres és folyamatos értékelését, a mutatók nyomon követését, a gyűjtött információ kiértékelését és a válaszüntézkedéseket írják elő, vagyis az 1.23. pont elemeit rendszerszinten ismétlik meg. A rendszerszintű stratégia rendszerenként, a rendszerbiztonsági terv részeként vagy mellékleteként készül. Középvállalatnál a két szint egy dokumentumban is kezelhető, ha a rendszerenkénti eltéréseket, például az eltérő osztályból adódó gyakoriságokat, külön táblázat rögzíti.

A kockázatmonitorozás a stratégia kötelező része, és a mutatók csoportosítását is megadja.

5.18. A szervezet biztosítja, hogy a kockázatmonitorozás szerves része legyen a folyamatos felügyeleti stratégiának, amely a következőket tartalmazza:

5.18.1. a hatékonyság ellenőrzését;

5.18.2. a megfelelés ellenőrzését; és

5.18.3. a változások nyomon követését. [7/2024. (VI. 24.) MK rendelet 2. melléklet 5.18. pont] (A, J, M)

A hatékonysági mutató azt méri, hogy a kontroll eléri-e a célját, a megfelelési mutató azt, hogy a szabályzat szerint működik-e, a változáskövetési mutató pedig azt, hogy a rendszer mennyiben tér el a jóváhagyott állapottól.

A további kiegészítések osztályfüggők. A független értékelők alkalmazása jelentős és magas osztályban kötelező. A trendelemzés és a felügyelet automatizált támogatása egyik osztályban sem kötelező, a monitoring rendszerrel rendelkező Szervezetnél azonban kis ráfordítással teljesíthető.⁵

4.2.4 A kapcsolódó követelmények

A folyamatos felügyelet adatforrásait más követelménycsoportok írják elő. A naplóbejegyzések felülvizsgálata, elemzése és jelentése minden osztályban kötelező, az automatizált folyamatintegráció és a naplózási tárhelyek összekapcsolása jelentős osztálytól. További adatforrás a sérülékenységek ellenőrzése, az EIR monitorozása és az események majdnem valós idejű automatizált elemzése.

Az intézkedési terv frissítésénél a rendelet kifejezetten a folyamatos felügyeleti tevékenységek eredményeire hivatkozik [5.10.2. pont] (A, J, M).⁶ A stratégia ezeket nem ismétli meg, hanem hivatkozik rájuk, és meghatározza, milyen mutató készül az adataikból.

A fogalmi elhatárolás a gyakorlatban is számít. A „monitorozás” (18.13. pont) technikai tevékenység, a támadások és a jogosulatlan használat észlelése. A „folyamatos felügyelet” irányítási tevékenység, a védelmi intézkedések hatékonyságának mérése és jelentése, amelynek a technikai monitorozás csak az egyik adatforrása. A monitoring rendszer megléte ezért nem azonos a stratégia meglétével, hiánya pedig nem mentesít az elkészítése alól.

4.3 Milyen szabványok segítik az értelmezést

4.3.1 A NIST kiadványok

A rendelet védelmi intézkedés katalógusa a Nemzeti Kibervédelmi Intézet alkalmazási útmutatója szerint a NIST SP 800-53 Rev. 5 kontrollkatalógusra épül.⁷ A megfeleltetés a folyamatos felügyeletnél pontról pontra követhető. Az 1.23. pont a PM-31 (Continuous Monitoring Strategy), az 5.15. pont a CA-7 (Continuous Monitoring) kontroll fordítása, az 5.16., 5.17., 5.18., 5.19. és 5.20. pont pedig rendre a CA-7(1), CA-7(3), CA-7(4), CA-7(5) és CA-7(6)

⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 5.16. pont (J, M), 5.17. pont (O), 5.19. pont (O) és 5.20. pont (O)

⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 4.13.1. és 4.13.2. pont (A, J, M), 4.14. és 4.15. pont (J, M), 15.9. pont (A, J, M), 18.13. pont (A, J, M), 18.15. pont (J, M), 5.10.2. pont (A, J, M)

⁷ NBSZ Nemzeti Kibervédelmi Intézet, Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, 1.0 verzió (2024. augusztus), nki.gov.hu

kontrollkiegészítés. Az 1. melléklet 1.1.7. pontja a NIST SP 800-37 Rev. 2 kockázatmenedzsment keretrendszer hetedik, „Monitor” lépésének felel meg. A jogszabály egy-egy fordulatanak jelentését ezért a NIST SP 800-53 Rev. 5 megfelelő kontrolljának magyarázó („Discussion”) része adja meg.⁸

A folyamatos felügyeleti program módszertanát a NIST SP 800-137 írja le hatlépéses folyamatként, a stratégia meghatározása, a program felállítása a mutatókkal és a gyakoriságokkal, a végrehajtás, az elemzés és jelentés, a válaszlépések, végül a stratégia felülvizsgálata. Ez a hat lépés az 1.23. pont hat elemével lényegében azonos, ezért a rendelet olvasásához ez a legfontosabb háttéranyag. A program érettségének értékeléséhez a NIST SP 800-137A ad módszert.⁹ A mérőszámok kialakításához a NIST SP 800-55 2024 decemberében megjelent két kötete az irányadó, az első a mutatók azonosítását és kiválasztását, a második a mérési program felépítését tárgyalja, a mutatókat megvalósítási, hatékonysági és hatás típusra osztja, és sablont ad a leírásukhoz.¹⁰ A naplókezeléshez a NIST SP 800-92, a technikai észleléshez a NIST kiberbiztonsági keretrendszer 2.0 DE.CM kategóriája ad támpontot.¹¹

4.3.2 Az ISO szabványok

Az ISO/IEC 27001 (2022) szerint tanúsított vagy arra készülő Szervezet a rendelet követelményét a szabvány 9.1. pontjával feleltetheti meg. A szabvány itt azt várja el, hogy a szervezet határozza meg, mit, milyen módszerrel, mikor és ki figyel és mér, mikor és ki elemzi és értékeli az eredményeket, és őrizze meg az eredmények bizonyítékát. Ez tartalmilag ugyanaz, mint az 1.23. pont hat eleme, a belső audit (9.2.) és a vezetőségi átvizsgálás (9.3.) pedig a rendelet jelentési és válaszlépési elemének felel meg. A mutatók kialakításához az ISO/IEC 27004 (2016) ad módszertant és a B mellékletében példákat, többek között a naplóátvizsgálásra, a sérülékenységek javítására és az incidenskezelés hatékonyságára, a kontrollszintű tartalmat pedig az ISO/IEC 27002 (2022) naplózási, felügyeleti és sérülékenységkezelési pontjai adják.¹²

4.3.3 Az uniós források és az egyéb ajánlások

A NIS2 irányelv a kockázatkezelési intézkedések hatékonyságának értékelésére szolgáló szabályzatokat és eljárásokat a minimumintézkedések közé sorolja, a rendelet folyamatos felügyeleti követelménye ennek hazai megjelenése. A digitális infrastruktúra egyes szolgáltatóira közvetlenül alkalmazandó (EU) 2024/2690 bizottsági végrehajtási rendelet mellékletének 7. pontja a hatékonyságértékelés tartalmát részletezi, az ENISA 2025 júniusi technikai végrehajtási útmutatója pedig példákat és elvárt bizonyítékokat sorol fel hozzá. Más ágazatban működő Szervezet számára ez nem kötelező, az elvárás értelmezéséhez azonban jó minta.¹³ A CIS Controls v8.1 hetedik (sérülékenységkezelés), nyolcadik (naplókezelés) és tizenharmadik

⁸ NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations (2020, frissítve 2023), PM-31 és CA-7 kontroll; NIST SP 800-37 Rev. 2, Risk Management Framework (2018), Monitor lépés

⁹ NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (2011), 3. fejezet; NIST SP 800-137A, Assessing ISCM Programs (2020)

¹⁰ NIST SP 800-55 Vol. 1, Measurement Guide for Information Security, Identifying and Selecting Measures, és Vol. 2, Developing an Information Security Measurement Program (2024. december)

¹¹ NIST SP 800-92, Guide to Computer Security Log Management (2006. szeptember); NIST Cybersecurity Framework 2.0 (2024. február), DE.CM kategória

¹² ISO/IEC 27001 (2022), 9.1., 9.2., 9.3. és 10.1. pont, A melléklet 5.36., 8.8., 8.15. és 8.16. kontroll; ISO/IEC 27004 (2016), B melléklet; ISO/IEC 27002 (2022), 5.36., 8.8., 8.15. és 8.16. pont

(hálózati felügyelet) kontrollja megvalósítási csoportonként ad minimumot, ezért közép vállalatnál a célértékek megállapításához jól használható.¹⁴

4.4 A stratégia ajánlott tartalma és mérőszámai közép vállalatnál

4.4.1 A mindkét esetben szükséges elemek

A jogszabály hat, illetve hét kötelező elemét a Gyakorlati javaslatok fejezetben leírt öt fejezet fedi le. A mutatók kiválasztásánál a NIST SP 800-55 három típusát érdemes vegyíteni. A megvalósítási mutató azt mutatja, hol tart egy kontroll bevezetése (például a többtényezős hitelesítés lefedettsége), a hatékonysági mutató azt, hogy a kontroll működik-e (például a javítási átfutási idő), a hatásmutató pedig az üzleti következményt. Közép vállalatnál az első két típus a hangsúlyos, hatásmutatóból egy vagy kettő elegendő. A célértéket a Szervezet első alkalommal a próbaüzem adatai alapján állítja be, majd évente szigorítja. Az incidensekhez kapcsolódó időmutatóknál a jogszabályi bejelentési határidők, a tudomásszerzéstől számított 24 és 72 óra, adják a külső korlátot.¹⁵

4.4.2 Ha a Szervezet monitoring és logelemző rendszert használ

Mutató	Adatforrás	Gyakoriság	Javasolt célérték
Naplóforrás-lefedettség, bekötött rendszerelemek aránya	SIEM, EIR-nyilvántartás	havi	legalább 95%
Néma naplóforrások, 24 órán túl nem küldő	SIEM állapotjelentés	napi	0
Riasztások tudomásulvételi és lezárási ideje súlyosság szerint	SIEM, hibajegy	havi	kritikusnál 1 óra és 1 munkanap
Kritikus és magas sérülékenységek javítási átfutási ideje	sérülékenységszkenner	havi	14, illetve 30 nap
Végpontvédelem lefedettsége, aktív ügynökök	EDR konzol, eszköztár	havi	legalább 98%
Többtényezős hitelesítés lefedettsége, inaktív és privilegizált fiókok	címár, identitásszolgáltató	havi	100%, felülvizsgált
Nem engedélyezett konfigurációváltozások száma	SIEM, változáskezelés	havi	0
Mentés sikeressége és helyreállítási teszt	mentőrendszer	heti, félévente	100% és sikeres teszt
Incidensek száma és a bejelentési határidő betartása	incidensnyilvántartás	negyedéves	100% határidőn belül
Képzés teljesítése és adathalász-teszt kattintási aránya	oktatási nyilvántartás	negyedéves	100% és 5% alatt
Intézkedési terv határidőn túli tételei	intézkedési terv	negyedéves	0

Ilyen eszközkörnyezetben az 5.17. pont szerinti trendelemzés és az 5.20. pont szerinti automatizált támogatás a rendszer irányítópultjával teljesül. A független értékelést (5.16. pont) a jelentős és magas osztályú rendszereknek az üzemeltetéstől független szereplő (például független belső auditor vagy külső értékelő) évenkénti bevonásával kell biztosítani.

4.4.3 Ha a Szervezet nem használ monitoring és logelemző rendszert

A stratégia ugyanazt a hat elemet tartalmazza, a mutatók száma tíz körüli, és minden mutatóhoz kézi gyűjtési lépés és felelős tartozik.

¹³ (EU) 2022/2555 irányelv 21. cikk (2) bekezdés f) pont; a Bizottság (EU) 2024/2690 végrehajtási rendelete (2024. október 17.), melléklet 7. pont; ENISA, Technical implementation guidance on cybersecurity risk management measures, 1.0 verzió (2025. június)

¹⁴ CIS Critical Security Controls v8.1 (2024. június), 7., 8. és 13. kontroll

¹⁵ 418/2024. (XII. 23.) Korm. rendelet 77. § (1) bekezdés 1. és 3. pont

Mutató	Adatforrás	Gyakoriság	Javasolt célérték
Naplóátvizsgálások teljesítése, elvégzett és előírt átnézés aránya	ellenőrzési naptár, jegyzőkönyv	heti, havi	100%
Biztonsági frissítések és végpontvédelem állapota	frissítéskezelő, védelmi konzol	havi	95% 30 napon belül, 98% lefedettség
Nyitott kritikus és magas sérülékenységek száma és kora	negyedéves szkennelés jelentése	negyedéves	0 kritikus 30 napon túl
Többtényezős hitelesítés lefedettsége	cím tár, felhőszolgáltató konzol	negyedéves	100% távoli hozzáférésnél
Inaktív és privilegizált fiókok száma	cím táreexport	negyedéves	felülvizsgált, dokumentált
Mentés sikeressége és helyreállítási teszt	mentési napló	heti, félévente	100% és sikeres teszt
Incidensek és incidensközeli helyzetek száma, határidők	incidensnyilvántartás	negyedéves	100% határidőn belül
Képzés teljesítése	oktatási nyilvántartás	félévente	100%
Intézkedési terv határidőn túli tételei	intézkedési terv	negyedéves	0

A kézi módszer jogi korlátja a biztonsági osztály. Alap osztályú rendszernél a 4.13. pont szerinti felülvizsgálat kézi átnézéssel is teljesíthető, ha a gyakoriság és az eredmény dokumentált. Jelentős vagy magas osztállynál a 4.14., a 4.15. és a 18.15. pont automatizált mechanizmust, a naplótárak összekapcsolását és közel valós idejű elemzést kíván, ezt kézi átnézés nem pótolja. Ilyenkor a hiányt az intézkedési tervben mérföldkövel és határidővel kell rögzíteni, az addig alkalmazott sűrített kézi átnézés és a külső szolgáltató bevonását pedig a rendelet 1. melléklet 3.1.2. pontja szerint eltérésként dokumentálni és jóváhagyatni.

A stratégia tartalmi hiányát az auditor az alábbi kérdésekkel tárhatja fel:

- Vannak-e számszerű mutatók?
- Készül-e róluk időszakos jelentés?
- Született-e a jelentés alapján intézkedés?

Ha bármelyikre nemleges a válasz, a folyamatos felügyelet csak papíron létezik, és a vezető 6. § (3) bekezdés 10. pontja szerinti kötelezettségének teljesítése sem igazolható.

5. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról; 7/2024. (VI. 24.) MK rendelet; 418/2024. (XII. 23.) Korm. rendelet; (EU) 2022/2555 irányelv (NIS2); (EU) 2024/2690 bizottsági végrehajtási rendelet
- NIST SP 800-53 Rev. 5, SP 800-37 Rev. 2, SP 800-137, SP 800-137A, SP 800-55 Vol. 1 és 2, SP 800-92, CSF 2.0; ISO/IEC 27001 (2022), 27002 (2022), 27004 (2016); CIS Controls v8.1; ENISA technikai végrehajtási útmutató (2025); NKI alkalmazási útmutató (2024)