A Kiberbiztonsági törvény szerinti sérülékenységvizsgálat, valamint a védelmi intézkedések keretében végzett technikai vizsgálatok (sérülékenységkeresés, behatolásvizsgálat) elhatárolása és jogi háttere

VFP2 KiberVéd - NIS2 Audit felkészítés – MKIK Iránymutatás 2026/6

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.30	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Jelen dokumentum célja, hogy közérthető formában különbséget tegyen a technikai vizsgálati típusok és a formális hatósági vizsgálat között, és egyértelművé tegye a szervezetek jogi kötelezettségeit.

Az írás összefoglalja, hogy a magyar kiberbiztonsági szabályozás, különösen a 2024. évi LXIX. törvény, a 418/2024. (XII. 23.) Korm. rendelet és a 7/2024. (VI. 24.) MK rendelet alapján

- mikor kötelező sérülékenységkeresést, behatolásvizsgálatot és jogi értelemben vett sérülékenységvizsgálatot végezni vagy végeztetni,
- mely szervezetek és szakemberek jogosultak sérülékenységvizsgálat lefolytatására,
- milyen esetekben rendelheti el a nemzeti kiberbiztonsági hatóság utóvizsgálat lefolytatását.

Az útmutató kiemelt figyelmet fordít a szervezetek biztonsági osztályba sorolásából (Alap, Jelentős, Magas) fakadó eltérő kötelezettségekre, valamint a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) és a Nemzeti Kiberbiztonsági Hatóság (NBSZ NKI) hatásköreinek elhatárolására, biztosítva a jogi megfelelést és a bírságkockázatok minimalizálását.

2. A VIZSGÁLANDÓ TERÜLET

Milyen szervezetek számára kötelező a sérülékenységvizsgálat?

Ki végezhet sérülékenységvizsgálatot?

3. VÁLASZ

3.1 Milyen szervezetek számára kötelező a sérülékenységvizsgálat?

A sérülékenységvizsgálat kötelezettsége alapvetően az alábbi esetben merül fel:

A Kiberbiztonsági tv. 57. §-a szerinti, formális sérülékenységvizsgálat lefolytatása kötelező, amennyiben azt a Nemzeti Kiberbiztonsági Hatóság (vagy honvédelmi rendszerek esetén a KNBSZ) hatósági döntésben, felügyeleti eljárás keretében, vagy a 418/2024. (XII. 23.) Korm. rendelet 87. §-a szerinti incidenskezelés során elrendeli.

Ezzel szemben a 7/2024. (VI. 24.) MK rendelet szerinti behatolásvizsgálat és sérülékenységkeresés hatósági határozat nélkül is kötelező védelmi intézkedés: a sérülékenységkeresés minden osztályban rendszeresen, míg a behatolásvizsgálat a 'Magas' biztonsági osztályba sorolt rendszerek esetében előírt gyakorisággal végzendő.

Fontos, hogy különbséget tegyünk a sérülékenységkeresés (sérülékenység szkennelés), a behatolásvizsgálat (penetration test) és a jogi értelemben vett sérülékenységvizsgálat között.

A 7/2024. (VI. 24.) MK rendelet elsősorban a sérülékenységkeresésre és behatolásvizsgálatra vonatkozó védelmi intézkedéseket írja elő, míg a 2024. évi LXIX. törvény a sérülékenységvizsgálatot mint hatósági felügyelet mellett zajló, formális eljárást szabályozza.

3.2 Ki jogosult sérülékenységvizsgálat elvégzésére

A 2024. évi LXIX. törvény (Kiberbiztonsági tv.), valamint a végrehajtására kiadott kormányrendeletek szigorúan szabályozzák, hogy mely szervezetek és személyek jogosultak sérülékenységvizsgálat elvégzésére. A szabályozás célja, hogy garantálja a vizsgálatot végzők szakmai kompetenciáját és megbízhatóságát, tekintettel az érintett rendszerek kritikus jellegére.

A jogszabályi keretek alapján a jogosultak köre három fő kategóriára osztható: állami szervek, a honvédelmi ágazat speciális szervei, valamint a piaci szereplők (gazdálkodó szervezetek).

A törvény értelmében sérülékenységvizsgálatot kizárólag az alábbi három kategóriába tartozó szervezet végezhet:

- Kijelölt állami szerv, a honvédelmi célú rendszerek kivételével ez a szerv látja el az állami szférát érintő vizsgálatokat. A Kormány ezt a feladatot a Nemzetbiztonsági Szakszolgálatra (NBSZ) delegálta.
- Honvédelmi kiberbiztonsági incidenskezelő központ, kizárólag a honvédelmi célú elektronikus információs rendszerek vonatkozásában rendelkezik jogosultsággal. Ezt a feladatot a Katonai Nemzetbiztonsági Szolgálat (KNBSZ) látja el.
- Jogosult gazdálkodó szervezet, olyan piaci szereplő, amely rendelkezik a megfelelő tanúsítványokkal (telephely biztonsági tanúsítvány), infrastrukturális feltételekkel, szakértelemmel, és szerepel az SZTFH által vezetett nyilvántartásban.

A Kiberbiztonsági tv. vonatkozó rendelkezéseinek pontos szövege:

> *„(1) Sérülékenységvizsgálat végzésére jogosult*
> *a) a honvédelmi célú elektronikus információs rendszerek kivételével a Kormány rendeletében kijelölt állami szerv,*
> *b) a honvédelmi célú elektronikus információs rendszerek vonatkozásában a honvédelmi kiberbiztonsági incidenskezelő központ, valamint*
> *c) a telephely biztonsági tanúsítvánnyal, továbbá a feladat ellátásához szükséges infrastrukturális feltételekkel és szakértelemmel rendelkező azon gazdálkodó szervezet, amely szerepel a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetek SZTFH által vezetett nyilvántartásában.”*
> *[2024. évi LXIX. törvény 57. § (1) bekezdés]*

A 418/2024. (XII. 23.) Korm. rendelet pontosítja az állami és honvédelmi feladatellátókat:

> *„(1) A Kormány a Kiberbiztonsági tv. 57. § (1) bekezdés a) pontja szerinti állami szervként a Nemzetbiztonsági Szakszolgálatot jelöli ki (a továbbiakban: sérülékenységvizsgálat végzésére jogosult állami szerv).*

(2) A honvédelmi célú elektronikus információs rendszerek vonatkozásában a sérülékenységvizsgálat lefolytatására a Katonai Nemzetbiztonsági Szolgálat jogosult."
[418/2024. (XII. 23.) Korm. rendelet 48. § (1)-(2) bekezdés]

Nem elegendő, ha maga a cég rendelkezik jogosultsággal. A vizsgálatot ténylegesen végrehajtó szakértőnek is szigorú, személyhez kötött feltételeknek kell megfelelnie. A sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetek és természetes személyek nyilvántartásáról és a velük szemben támasztott követelményekről szóló 5/2025 (VI.20.) SZTFH rendelet alapján a vizsgálatot a gazdálkodó szervezet részéről csak olyan személy végezheti, aki

- rendelkezik a sérülékenységvizsgálat lefolytatásához szükséges szakértelemmel és – a végrehajtási rendeletben meghatározottak szerint – megfelelő végzettséggel, vagy
- a sérülékenységvizsgálati szakterületen legalább kétéves szakmai tapasztalattal rendelkezik,
- szerepel a sérülékenységvizsgálat lefolytatására jogosult személyek SZTFH által vezetett nyilvántartásában.

„(2) A sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezet részéről kizárólag olyan személy végezheti a vizsgálatot, aki
a) rendelkezik a sérülékenységvizsgálat lefolytatásához szükséges szakértelemmel,
b) a sérülékenységvizsgálati szakterületen legalább kétéves szakmai tapasztalattal rendelkezik, és
c) szerepel a sérülékenységvizsgálat lefolytatására jogosult személyek SZTFH által vezetett nyilvántartásában."
[2024. évi LXIX. törvény 57. § (2) bekezdés]

A megbízó szervezet felelőssége, hogy a szerződéskötés előtt ellenőrizze ezen jogosultságok meglétét.

3.3 Mikor kötelező az állami szervet (NBSZ-NKI) igénybe venni?

Főszabály szerint az érintett szervezetek (például alapvető és fontos szervezetek) a jogszabályban meghatározott feltételeknek megfelelő, az SZTFH által nyilvántartásba vett gazdálkodó szervezetek közül választhatnak a sérülékenységvizsgálat elvégzésére.

Ha azonban nincs olyan gazdálkodó szervezet, amely megfelel a törvényben előírt követelményeknek, a sérülékenységvizsgálatot a Kormány által kijelölt állami szerv, azaz a Nemzetbiztonsági Szakszolgálat végzi el.

Vannak azonban kivételes esetek, amikor a vizsgálatot kizárólag a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (mint kijelölt állami szerv) végezheti el. Ez akkor fordul elő, ha egy kritikus vagy az ország biztonsága szempontjából jelentős szervezet rendszerét kell vizsgálni, és nincs a piacon olyan gazdálkodó szervezet, amely megfelelne az adott vizsgálathoz szükséges feltételeknek.

„(7) A sérülékenységvizsgálatot a sérülékenységvizsgálat végzésére jogosult állami szerv végzi el, ha az (5) bekezdés a) pontja szerinti elektronikus információs rendszereken kívüli, a Kszetv. szerinti kritikus szervezet, valamint a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölt szervezet elektronikus információs rendszere tekintetében nincs a sérülékenységvizsgálat elvégzésére e törvényben meghatározott feltételeknek megfelelő, sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezet.” [2024. évi LXIX. törvény 57. § (7) bekezdés]

4. A SÉRÜLÉKENYSÉG SZKENNELÉS, BEHATOLÁSVIZSGÁLAT ÉS SÉRÜLÉKENYSÉGVIZSGÁLAT FOGALMAK ELHATÁROLÁSA

A három fogalom – sérülékenység szkennelés, behatolásvizsgálat és sérülékenységvizsgálat – a köznapi nyelvben gyakran összemosódik, azonban jogi és műszaki szempontból élesen elkülönülő tevékenységeket takarnak. A legfontosabb különbség a vizsgálat mélységében, módszertanában és a jogszabályi kötelezettség jellegében ragadható meg.

4.1 Sérülékenység szkennelés (sérülékenységkeresés)

Ez a folyamat jellemzően automatizált eszközökkel végzett, rendszeres technikai ellenőrzést jelent. A célja a rendszerben lévő ismert technikai hiányosságok (pl. elavult szoftververziók, hiányzó frissítések, alapértelmezett jelszavak) gyors azonosítása anélkül, hogy azokat a vizsgálat során ténylegesen kihasználnák.

A 7/2024. (VI. 24.) MK rendelet „Sérülékenységkezelés” cím alatt írja elő ezt a tevékenységet. Jogszabályi terminológiában ez „sérülékenységkeresésként” jelenik meg. Ez egy alapvető higiéniai intézkedés, amelyet a szervezetnek folyamatosan vagy rendszeres időközönként kell végeznie. Ez nem azonos a Kiberbiztonsági törvény szerinti, formális sérülékenységvizsgálattal.

„5.14. A szervezet rendszeres időközönként sérülékenységkeresést végez az összes EIR és rendszerelem tekintetében a potenciális sebezhetőségek azonosítása érdekében, valamint naprakészen tartja a sérülékenységekkel kapcsolatos információkat.”
„5.15. A szervezet meghatározza a sérülékenységkeresés végrehajtásának gyakoriságát, az alkalmazott módszereket és az érintett rendszerelemeket.” [7/2024. (VI. 24.) MK rendelet 2. melléklet 5.15. pont (A, J, M)]

A fejlesztések során a szoftverfejlesztői tesztelés keretében is kötelező a biztonsági vizsgálat a Jelentős és Magas biztonsági osztályoknál:

16.66. A szervezet az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől megköveteli, hogy:...
16.66.2. Meghatározott gyakorisággal hajtson végre (a fejlesztéshez illeszkedő módon) egység-, integrációs-, rendszer-, illetve regressziós

tesztelést, és értékelje ki a szervezet által meghatározottak szerint.
[7/2024. (VI. 24.) MK rendelet 2. melléklet (A, J, M)]

4.2 Behatolásvizsgálat (Penetration testing)

A behatolásvizsgálat (etikus hackelés) egy mélyebb, célorientált vizsgálat. Itt nemcsak a hibák listázása a cél, hanem annak szimulálása, hogy egy rosszindulatú támadó hogyan tudná ezeket a hibákat kihasználni (exploitálni) a védelmi vonalak áttörésére. Ez a vizsgálat emberi szakértelmet igényel, és bizonyítja a védelmi intézkedések tényleges hatékonyságát.

A védelmi intézkedések katalógusában a behatolásvizsgálat kötelezősége az egyes biztonsági osztályoknál eltérő; „Magas" osztály esetén kötelező védelmi intézkedés, míg „Alap" és „Jelentős" osztályban opcionálisan, szervezet által meghatározott kockázatarányos módon alkalmazható. Magas biztonsági osztály esetében külső, független szakértőt kell bevonni.

„5.21. A szervezet behatolásvizsgálatot végez a szervezet által meghatározott gyakorisággal a meghatározott EIR-eken vagy rendszerelemeken.(O)
5.22. A szervezet független szakértőt vagy csapatot alkalmaz az EIR vagy a rendszerelemek behatolásvizsgálatának elvégzésére"(M)
[7/2024. (VI. 24.) MK rendelet 2. melléklet 5.21. pont]

Bár nem a szervezet végzi, de a szervezet köteles tűrni és támogatni a kétévente esedékes kiberbiztonsági auditot, amelynek során az auditor jogosult technikai vizsgálatokat végezni.

A Kiberbiztonsági tv. 22. § (1) bekezdése szerinti megfelelőség ellenőrzésére az auditor jogosult a tevékenység nyomon követésére alkalmas módon a következőket elvégezni:

a) külső informatikai biztonsági és távoli sérülékenységvizsgálatot, valamint „jelentős" vagy „magas" biztonsági osztály esetén behatolásvizsgálatot,

4.3 Sérülékenységvizsgálat (Jogi értelemben)

A magyar jogi terminológiában a „sérülékenységvizsgálat" a 2024. évi LXIX. törvény (Kiberbiztonsági tv.) által definiált, formális eljárás. Ez nem csupán technikai tesztelést jelent, hanem egy hatósági felügyelet mellett zajló, hatósági nyilvántartásban szereplők (vagy az NBSZ) által végzett átfogó auditot, amely magában foglalhatja a fenti technikai elemeket (szkennelés, behatolásvizsgálat) is, de jogi következményekkel és jelentéstételi kötelezettséggel jár.

Ez a fogalom a törvényben, mint szabályozott tevékenység jelenik meg, amelyet csak engedéllyel rendelkező szervezet végezhet.

„(1) Az érintett szervezet [...] köteles a biztonsági osztályba sorolást és a sérülékenységvizsgálatot elvégezni vagy elvégeztetni."
[2024. évi LXIX. törvény 7. § (1) bekezdés]
„(1) Sérülékenységvizsgálat végzésére jogosult [...] c) a telephely biztonsági tanúsítvánnyal, továbbá a feladat ellátásához szükséges infrastrukturális feltételekkel és szakértelemmel rendelkező azon

gazdálkodó szervezet, amely szerepel a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetek SZTFH által vezetett nyilvántartásában." [2024. évi LXIX. törvény 57. § (1) bekezdés]

4.4 Összehasonlító táblázat

Szempont	Sérülékenységkeresés (Scanning)	Behatolásvizsgálat (Pentest)	Sérülékenységvizsgálat (Törvényi eljárás)
Cél	Ismert hibák automatizált, gyors felderítése.	Védelmi rendszer áttörésének szimulációja, emberi intelligenciával.	Jogszabályi megfelelés igazolása, átfogó biztonsági állapotfelmérés, hatósági kontroll.
Módszertan	Automatizált szoftveres feltérképezés (pl. MKIK Securebot, - **https://kiberbiztonsag.mkik.hu/** Nessus, OpenVAS).	Manuális és automatizált támadási szimuláció, social engineering.	Komplex audit (adminisztratív + technikai vizsgálat) szigorú protokoll szerint.
Végrehajtó	Belső üzemeltetés vagy szoftver.	Etikus hacker (belső vagy külső). Magas osztályban kötelezően független.	Kizárólag jogszabályban feljogosított szerv (NBSZ, KNBSZ) vagy TBT-vel és SZTFH regisztrációval rendelkező cég.
Jogi hivatkozás	7/2024. (VI. 24.) MK rendelet 2. melléklet 5.14–5.15. pont [8]	7/2024. (VI. 24.) MK rendelet 2. melléklet 5.21–5.22. pont; Kiberbiztonsági tv. 22. §	2024. évi LXIX. törvény 57. §, 62–64. §
Gyakoriság	Rendszeres (pl. havonta, negyedévente) – Folyamatos intézkedés.	Eseti vagy időszakos (pl. évente, vagy jelentős változáskor) – Kockázatarányos.	Eseti jelleggel: Hatósági kötelezésre, incidens kivizsgálása során, vagy a szervezet saját döntése alapján. (Nem azonos a 2 éves Audittal!)

5. MIKOR KÖTELEZŐ A SÉRÜLÉKENYSÉGVIZSGÁLAT?

5.1 Hatósági kötelezés alapján

A felügyeleti hatóság (Nemzetbiztonsági Szakszolgálat vagy a Honvédelmi Kiberbiztonsági Hatóság) eljárása során bármikor elrendelheti a sérülékenységvizsgálatot, ha azt indokoltnak

látja, például egy incidens kivizsgálása során, vagy ha a szervezet nem tesz eleget védelmi kötelezettségeinek a Kiberbiztonsági tv. 58.(1) bekezdés értelmében.

> *A nemzeti kiberbiztonsági hatóság a szervezetet kötelezheti arra, hogy sérülékenységvizsgálatot végeztessen.*

Továbbá Nemzeti Kiberbiztonsági Incidenskezelő Központ (NKIK)[1] is kezdeményezheti a vizsgálat elrendelését incidenskezelés, vagy vizsgálat során szerzett információk alapján, a 418/2024. (XII. 23.) Korm. rendelet 87. § (2) bekezdés alapján.

> *A Központ a kiberbiztonsági incidens kezelése, vizsgálata során tudomására jutott információk alapján kezdeményezheti a nemzeti kiberbiztonsági hatóságnál a kiberbiztonsági incidenssel érintett elektronikus információs rendszer sérülékenységvizsgálatának lefolytatására irányuló kötelezést.*

5.2 Utóvizsgálat kötelezettsége

Ha a sérülékenységvizsgálatról készült állásfoglalás kritikus vagy magas kockázati besorolású sérülékenységet állapít meg, a 2024. évi LXIX. törvény szerint utóvizsgálat lefolytatása kötelező. Az utóvizsgálat elrendeléséről és annak kötelező voltáról a nemzeti kiberbiztonsági hatóság dönt a sérülékenységvizsgálatot végző szerv állásfoglalása, valamint a szervezet által készített sérülékenységkezelési terv alapján.

Az utóvizsgálatot a szervezet a hatóság által jóváhagyott sérülékenységkezelési tervben meghatározott utolsó határidő leteltét követően kezdeményezi. A 2024. évi LXIX. törvény 64. § alapján.

> *Ha a sérülékenységvizsgálatot végző szerv az állásfoglalásban javaslatot tesz utóvizsgálat lefolytatására, a sérülékenységek megszüntetésére vonatkozó sérülékenységkezelési tervre irányuló döntésében a nemzeti kiberbiztonsági hatóság nyilatkozik, kötelezi-e utóvizsgálat elvégzésére a szervezetet.*
> *(2) Ha az állásfoglalás kritikus vagy magas besorolású sérülékenységet állapít meg, utóvizsgálat lefolytatása kötelező.*
> *(3) Kötelezően elvégzendő utóvizsgálat esetén a szervezet a nemzeti kiberbiztonsági hatóság által jóváhagyott sérülékenységkezelési tervben szereplő, utolsóként teljesítendő határidő leteltét követően kezdeményezi az utóvizsgálatot.*
> *(4) A szervezet az utóvizsgálatot saját maga is kezdeményezheti, ez esetben a kezdeményezéssel egyidejűleg – amennyiben erre még a kezdeményezést megelőzően nem került sor – megküldi a sérülékenységkezelési tervet a nemzeti kiberbiztonsági hatóság részére.*

[1] A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet keretei között működik.

(5) Utóvizsgálat lefolytatására a sérülékenységkezelési terv kiberbiztonsági hatóság általi jóváhagyását követően vagy indokolt esetben a nemzeti kiberbiztonsági hatóság engedélyét követően kerülhet sor.

A 418/2024. Korm. rendelet lehetőséget ad a kockázatok elfogadására. A sérülékenységvizsgálatról készült állásfoglalás kézhezvételét követő 30 napon belül a szervezetnek sérülékenységkezelési tervet kell készítenie, és azt jóváhagyásra megküldeni a Nemzeti Kiberbiztonsági Hatóságnak.

- A kritikus és magas kockázati besorolású sérülékenységek javítása és utóvizsgálata kötelező.
- Az alacsony és közepes kockázatú sérülékenységek esetében a szervezet dönthet a kockázat felvállalása mellett, amennyiben a javítás aránytalan terhet jelentene, és a kockázat menedzselhető. Ezt a tervben indokolni szükséges (alacsony kockázatnál az indokolás egyszerűsített lehet).

Az utóvizsgálat lefolytatására kizárólag a Hatóság által jóváhagyott terv birtokában, az abban szereplő határidők letelte után kerülhet sor

6. FORRÁSOK

1. 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

2. 418/2024. (XII. 23.) Korm. rendelet a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

3. 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

4. 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról

5. 5/2025 (VI.20.) SZTFH rendelet a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetek és természetes személyek nyilvántartásáról és a velük szemben támasztott követelményekről