Molnár Dóra✧

Mit mond a jog? Az elektronikus információs rendszerek fejlesztése

DOI 10.17047/HADTUD.2026.36.2.161

A magyar jogszabályi környezetben jelentős változások álltak be 2025. január 1-jével, amikor a korábbi (több esetben igencsak régi) jogszabályokat hatályon kívül helyezték, és olyan új jogszabályokat alkottak hazánkban, mint például a Magyarország kiberbiztonságáról szóló törvény. Mindez kihatott az elektronikus információs rendszerek fejlesztésére is, amelyekre vonatkozó jogszabályi környezetet nem csak az uniós előírásokhoz kellett hozzáigazítani, hanem az elmúlt években tapasztalt fejlődés következtébe megjelenő új igényekhez is. A tanulmány célja, hogy felvázolja az e fejlesztési folyamatra vonatkozó legfőbb jogszabályi előírásokat, kitérve a kötelező előírások és a hatósági jogkörök bemutatására is.

KULCSSZAVAK: elektronikus információs rendszer, fejlesztés, kiberbiztonság, Magyarország

What does Law Say? The Development of Electronic Information Systems

Significant changes took place in the Hungarian legal landscape on 1st January 2025, when previous (in many cases quite outdated) laws were repealed and new legislation was enacted, such as the Act on Cybersecurity in Hungary. All of this has also impacted the development of electronic information systems, for which the legal framework had to be adapted not only to EU provisions, but also to new demands arising from the developments of recent years. The aim of this study is to outline the main legal requirements pertaining to this development process, including a discussion of mandatory requirements and the competence of public authorities.

KEYWORDS: electronic information system, development, cybersecurity, Hungary

✧ Nemzeti Közszolgálati Egyetem (NKE), Hadtudományi és Honvédtisztképző Kar (HHK), Nemzetközi Biztonsági Tanulmányok Tanszék, egyetemi docens –
associate professor; Ludovika University of Public Service (UPS), Faculty of Military Sciences and Officer Training, International Security Policy Department;
e-mail: molnar.dora@uni-nke.hu, https://orcid.org/0000-0002-1476-5253

Bevezetés

2025. január 1-jével az elektronikus információs rendszerekre (a továbbiakban: EIR) vonatkozó szabályozás terén jelentős változás következett be. Ennek hátterében egyrészt az áll, hogy uniós tagállamként Magyarországon is implementálni kellett a magas szintű uniós kiberbiztonság megteremtése érdekében megalkotott ún. NIS 2 irányelvet,[1] másrészt szükségessé vált a korábbi jogszabály alkalmazási tapasztalatainak feldolgozása is.

A változás jelentős mértékben érintette a jogalkotást. A korábbi, központi jogszabályként funkcionáló törvényt[2] és kapcsolódó jogszabályokat[3] hatályon kívül helyezték, és azokat új jogforrások váltották fel. 2025. január 1-je óta a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kibertv.), valamint a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: Vhr.) tartalmazzák az új EIR bevezetése vagy már működő EIR továbbfejlesztése során alkalmazandó legfontosabb szabályokat.

A Kibertv. 4. § az értelmező rendelkezések körében rögzíti az elektronikus információs rendszer,[4] annak biztonsága[5] és továbbfejlesztése[6] fogalmát is.

Jelen tanulmány célja, hogy röviden bemutassa annak az általános eljárásrendnek a fő pontjait, amelyek az EIR-ek fejlesztése során a szervezet számára követendő. Terjedelmi okokból nem térek ki a minősített adatot kezelő és a honvédelmi célú EIR-ekre vonatkozó különös szabályokra.

Az EIR fejlesztésére vonatkozó szabályok

Az EIR fejlesztésével[7] összefüggő általános eljárásrendet a Kibertv. „Az elektronikus információs rendszer fejlesztése, továbbfejlesztése" címet viselő 9. alfejezete tartalmazza, míg ennek további részletezése a Vhr. II. fejezetének 10. alfejezetében található.

---

1 Ez az Európai Parlamentnek és a Tanácsnak 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 szóló 2022. december 14-i (EU) 2022/2555 irányelve.

2 Az állami és önkormányzati szervek információbiztonságáról szóló 2013. évi L. törvény (Ibtv.)

3 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről, 187/2015. (VII. 13.) Korm. rendelet az állami és önkormányzati szervek elektronikus információs rendszereinek biztonsági elvárásairól és a logikai védelmi intézkedésekről, 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információs rendszerei biztonsági osztályba sorolásának és a szervezet biztonsági szintbe sorolásának követelményeiről.

4 24. pont: *a)* az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat, *b)* minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy *c)* az *a)* és *b)* alpontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

5 25. pont: az elektronikus információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát.

6 96. pont: az érintett, már működő elektronikus információs rendszer olyan mértékű fejlesztése, amely funkcionalitásának érdemi megváltozásával jár, vagy védelmének elvárt erősségére hatással van.

EIR rendszer fejlesztési folyamat során mindvégig alapelvként követendő a *„security by design"* (beépített biztonság) elve, amelynek lényege, hogy adott rendszer megfelelő biztonsági szintjének eléréshez a biztonságot már a tervezés szakaszától kezdve szem előtt kell tartani, és annak a folyamat egészét tekintve vezérlő elvként kell funkcionálni.

A fejlesztés a tervezéssel kezdődik. A tervezési szakasz során kell lerakni az EIR alapjait: el kell végezni a rendszerben kezelni tervezett adatok osztályozását, az EIR biztonsági osztályba sorolását, majd ezt a nemzeti kiberbiztonsági hatóságnak (a továbbiakban: Hatóság) jóváhagyásra be kell nyújtani.[8] A jóváhagyás hatósági eljárásban valósul meg, amely során a Hatóság az adatosztályozást és a biztonsági szintbe sorolást felülbírálhatja.

Fontos további lépés a szerződéskötés az EIR fejlesztését végző szervezettel. A szerződésben rögzítenie kell a Hatóság által jóváhagyott osztályba soroláshoz kapcsolódó valamennyi információbiztonsági követelményt, amelyeket a szervezetnek a fejlesztés során mindvégig be kell tartatnia a fejlesztést végző szervezettel. Ennek egy lehetséges eszköze az információbiztonsági terv elkészítése, amely a biztonsági osztályba sorolás eredményétől függően rögzíti a rendszer kapcsán teljesítendő információbiztonsági kontrollokat. Ha a fejlesztés során bármikor olyan körülmény jut a szervezet tudomására, amely befolyásolja az érintett EIR biztonságát, a tervezési folyamat egyes lépéseit ismételten el kell végezni.

A tervezési fázishoz kapcsolódó feladatokat összegzi a következő oldalon látható táblázat.[9]

A fejlesztést a biztonsági osztályba[10] sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendeletben (a továbbiakban: MK rendelet) meghatározott védelmi követelményeknek megfelelően kell végrehajtani. A fejlesztés során a szervezetnek lehetőség van felülvizsgálatra: az adatosztályozás vonatkozásában akkor, ha az EIR-ben kezelendő adatok körében következik be változás, a biztonsági osztályba sorolás vonatkozásában pedig akkor, ha az EIR kockázati környezetében következik be változás. A felülvizsgálat eredményeként kapott besorolást a Hatóságnak jóváhagyásra ismét be kell nyújtani.

A fejlesztés során a megállapított biztonsági osztályhoz tartozó követelményeket a rendszer használatbavételéig teljesíteni kell. A szervezet vezetője csak akkor dönthet az EIR használatba vételéről, amennyiben a rendszer biztonsági osztályát a hatóság jóváhagyta és a biztonsági osztályhoz tartozó védelmi követelmények teljesültek. A döntéssel egyidejűleg az EIR adatait a Hatósághoz be kell jelentenie.

---

7 A továbbiakban az új elektronikus információs rendszerek fejlesztése és a már meglévő elektronikus információs rendszerek továbbfejlesztése két esetét új EIR fejlesztése címszó alatt együtt kezelem.

8 Belső fejlesztés esetén az erőforrások allokációját megelőzően, külső fejlesztés esetén az arra irányuló szerződés megkötését megelőzően úgy, hogy az információbiztonsági követelmények az EIR fejlesztésére irányuló szerződésbe rögzítésre kerüljenek, figyelembe véve a közbeszerzésekre vonatkozó jogszabályi rendelkezéseket is.

9 NKI 2026: 5

10 A korábbi szabályozás öt biztonsági osztályt különböztetett meg (1-5-ig skálázva), az új szabályok értelmében jelenleg három biztonsági osztály létezik: alap, jelentős és magas. További változás, hogy a biztonsági osztályba sorolást már nem háromévente, hanem kétévente felül kell vizsgálni.

Az elektronikus információs rendszerek tervezési feladatai

Fázis	*Feladat*	*Dokumentum*
specifikáció	adatkörök meghatározása	Előzetes biztonsági osztályba sorolás
	fenyegetettségek azonosítása	
	kockázatok meghatározása	
	előzetes biztonsági osztályba sorolás	
	biztonsági követelmények azonosítása	Információ-biztonsági terv
tervezés	védelmi intézkedések magas szintű tervezése	
	védelmi intézkedések alacsony szintű tervezése	Rendszerbiztonsági terv

Ha az EIR sérülékenységvizsgálata – jogszabály vagy a Hatóság döntése alapján – kötelező, a használatba vételi döntés további feltétele a feltárt sérülékenységek vonatkozásában készített sérülékenységkezelési terv Hatóság általi jóváhagyása. „Jelentős" és „magas" biztonsági osztályba tartozó EIR esetében kötelező a kormányrendelet szerinti teljes körű sérülékenységvizsgálat kezdeményezése.[11] Azonban a felesleges duplikációk elkerülése érdekében a kiberbiztonsági audit végeztetésére kötelezett szervezetek EIR-ei vonatkozásában nem áll fenn a sérülékenységvizsgálat elvégeztetésének kötelezettsége. A szervezetnek további kötelezettsége áll fenn a támogató rendszerei vonatkozásában: annak is az általa támogatott EIR-nek megfelelő szintű védelemben kell részesülnie.

Mindig fontos különválasztani a szervezetet és az általa üzemeltetett vagy fejlesztett rendszereket. Biztonsági osztálya ugyanis csak a szervezet egyes rendszereinek van, nem magának a szervezetnek, de a biztonsági osztályba sorolás elvégzése minden esetben a szervezet felelőssége. A szervezettel szemben támasztott alapvető követelmény, hogy az EIR-ben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményét (ez az ún. CIA-triád) a rendszer funkcióira tekintettel és azokhoz igazodó súllyal mindig érvényre juttassa. A biztonsági osztályba sorolást a két fő szempont mentén kell elvégezni: a kezelt adatok azonosítása[12] és az adott EIR funkciói. Az adatgazda[13] vagy az érintett rendszer biztonságáért felelős személy azonosítja a rendszer által feldolgozott, tárolt és továbbított adatok típusait, majd ezután mind az adatok, mind a rendszer tekintetében vizsgálja a bizalmasság, sértetlenség vagy rendelkezésre állás hatásértékét (alap, jelentős, magas).[14]

11 Ez alól a szervezet csak kormányrendeletben meghatározott, sérülékenységvizsgálat végzésére jogosult állami szerv döntése alapján mentesülhet.

12 A rendszer által feldolgozott, tárolt, továbbított adatok típusainak azonosítása és minden adattípus esetében az adat életciklusának minden egyes szakaszának azonosítása.

13 Az adatgazda annak a szervezeti egységnek a vezetője, ahová a jogszabály vagy közjogi szervezetszabályzó eszköz az adat kezelését rendeli, illetve, ahol az adat keletkezik.

14 A biztonsági osztályba sorolás elsődleges felelőse az adatgazda, de közvetlenül együtt kell működnie a felső vezetéssel, az információs rendszerek biztonságáért felelős személlyel és a szervezet adatvédelmi tisztviselőjével is.

Ha a hatóság nem ért egyet az adatosztályozás eredményével, kötelezheti a szervezetet az adatosztályozás felülvizsgálatára, ismételt elvégzésére. Az adatgazda (vagy az EIR biztonságáért felelős személy) a rendszer biztonsági osztályát a rendszerbiztonsági tervben dokumentálja, amelyben a végleges osztályozási döntésen kívül a biztonsági osztályba sorolást alátámasztó indokolást is szerepeltetni kell.[15] A biztonsági osztályba sorolás eredményét a szervezet vezetője hagyja jóvá, minden esetben hatáselemzés alapján.

Az MK rendelet rögzíti azokat a *védelmi intézkedéseket* is, amelyeket a szervezetnek be kell építenie a működésébe a rendszerek biztonsági környezetének kialakításához.[16] Ezektől a szervezet csak indokolt esetben térhet el. A rendszer biztonságáért felelős személy egyrészt kezeli a védelmi intézkedésektől való eltéréseket, meghatározza a helyettesítő intézkedéseket és a rendszerbiztonsági tervekben rögzíti a kapcsolatos információkat. Másrészt – az adatvédelmi tisztviselővel együtt – felel a rendszerbiztonsági tervek kidolgozásáért, karbantartásáért, és biztosítja, hogy a rendszert az elfogadott védelmi intézkedéseknek megfelelően telepítsék és üzemeltessék. Az eltéréseket tartalmazó dokumentumot a szervezet vezetője vagy a kockázatok felvállalására jogosult szerepkört betöltő személy hagyja jóvá.

A védelmi intézkedések bevezetésekor minden esetben értékelni kell, hogy azok a rendszer biztonságértékelési terve alapján megfelelnek-e a biztonsági céloknak. Új rendszerek esetében a védelmi intézkedéseket a rendszer életciklusának kezdeti szakaszaiban implementálják, míg a fejlesztés alatt álló rendszerek esetében egy kezdeti önértékelést kell végezni annak megállapítására, hogy milyen védelmi intézkedések vannak már érvényben, mielőtt újakat vezetnek be. A meglévő rendszereknél a rendszer életciklusának üzemeltetési/karbantartási szakaszában vezethetnek be új intézkedéseket, illetve frissítik a már meglévőket. Minden bevezetett védelmi intézkedést a szervezet által meghatározott gyakorisággal értékelni kell, jelentés formájában.

Az EIR fejlesztésének egy speciális állomása a *sérülékenységvizsgálat*, amely végzésére a – korábbi szabályokkal összhangban – a Nemzetbiztonsági Szakszolgálat jogosult. Sérülékenységvizsgálat megindítására háromféle módon kerülhet sor: a Hatóság általi kötelezéssel, a sérülékenységvizsgálat végzésére jogosult állami szerv kezdeményezésére, valamint a szervezet általi kezdeményezésre. (Ez utóbbira kizárólag a biztonsági osztályba sorolt és a Hatóság által nyilvántartásba vett EIR vonatkozásában kerülhet sor, annak tervezett kezdetét megelőzően legalább 60 nappal.) Új szabály, hogy a sérülékenységvizsgálat nem csak a teljes információs EIR-re, hanem az EIR egy részére vonatkozóan is kezdeményezhető. A sérülékenységvizsgálat körében sor kerülhet belső és külső informatikai biztonsági vizsgálatra, alkalmazásvizsgálatra, vezeték nélküli hálózat informatikai biztonsági vizsgálatára, valamint a kiber-fizikai rendszerek biztonsági vizsgálatára. A Vhr. a fő vizsgálati módszerek között nevesíti az automatizált sérülékenységfelderítés és -elemzést,

15 Az NKI által készített, az MK rendelet szerinti három biztonsági osztályhoz készített rendszerbiztonsági terv sablonokat külön dokumentumban csatolom. Ezek a rendszerbiztonsági tervhez kapcsolódó alapkövetelményeket határozzák meg, annak fejezeteit rögzítik, és rövid tartalommal segítik az egyes fejezetekhez kapcsolódó elvárások körvonalazását.

16 Az egyes biztonsági osztályokban alkalmazandó védelmi intézkedések részletes katalógusát az MK rendelet 2. sz. melléklete tartalmazza.

a pszichológiai manipulációs vizsgálatot, a behatolásvizsgálatot, a kriptográfiai megfelelőségvizsgálatot és forráskódvizsgálatot. A vizsgálat lefolytatása szigorú határidőkhöz és eljárásrendhez kötött.[17]

Az EIR fejlesztések ellenőrzésének kétévente visszatérő állomása a *kiberbiztonsági audit*, amely során az EIR-ek biztonsági osztályba sorolását, valamint a biztonsági osztályba sorolás szerinti védelmi intézkedések megfelelőségét ellenőrzik a független auditorok. Ennek során az auditorok jogosultak belső informatikai biztonsági és távoli sérülékenységvizsgálat, „jelentős" vagy „magas" biztonsági osztály esetén behatolásvizsgálat, kriptográfiai megfelelőségvizsgálat, valamint „jelentős" vagy „magas" biztonsági osztály esetén a kritikus biztonsági funkciókat végző egyedileg fejlesztett szoftverek biztonsági forráskódvizsgálatának lefolytatására.

A Hatóság feladat- és jogköre

További kapcsolódó kérdésként fontosnak tartom röviden bemutatni azt, hogy az EIR-ek (és a Kibertv. hatálya alá tartozó szervezetek) megfelelő működéséhez, működtetéséhez elengedhetetlen folyamatos felügyelet és ellenőrzés hogyan valósul meg a hatályos szabályok alapján.

A jogszabály a felügyeleti jogköröket a Vhr.-ben kijelölt nemzeti kiberbiztonsági hatósághoz, a Nemzetbiztonsági Szakszolgálathoz telepítette (a továbbiakban: Hatóság). Feladati között az Ibtv.-ben meghatározott feladatok mellett új, a NIS 2 irányelvből eredő feladatok is megjelentek. Ezek között szerepel – az EIR fejlesztésével összefüggésben – a teljesség igénye nélkül például a biztonsági osztályba sorolás, a védelmi intézkedések és az ehhez kapcsolódó eljárási szabályok teljesülésének ellenőrzése; a minimálisan elvárt védelmi intézkedések és esetlegesen további biztonsági követelmények meghatározása; az auditjelentést megalapozó bizonyítékok bekérése és a tartalmi felülvizsgálata; rendszeres, eseti és célzott biztonsági ellenőrzések végzése; az ellenőrzés során feltárt hiányosságok felszámolásához szükséges intézkedések elrendelése és ezek teljesülésének ellenőrzése; vagy az EIR-ek használatba vételének és meglévő EIR továbbhasználatának jóváhagyása során helyszíni ellenőrzés tartásai és sérülékenységvizsgálat elrendelése. A fenti feladatok közül kettő alapfeladatot emelek ki: az adatosztályozást és a biztonsági osztályba sorolást, amelyeket röviden a következőképpen mutatok be.

Ami az *adatosztályozást* illeti, a Hatóság az adatosztályozás eredményét a biztonsági osztályba sorolás megalapozottságának vizsgálatára irányuló eljárás keretében értékeli. Ha a vizsgálat eredménye alapján nem egyértelmű az adatosztályozás szerinti besorolás, a Hatóság eljárása keretében tisztázza, hogy a szervezet milyen és mekkora mennyiségű adatot kezel vagy tervez kezelni az EIR-ben. Ha a Hatóság nem ért egyet az adatosztályozás eredményével, kötelezheti a szervezetet az adatosztályozás felülvizsgálatára vagy ismételt elvégzésére. Ha a vizsgálat eredménye alapján az EIR-ben kezelt vagy kezelni tervezett adatok köre alapján azok külföldi kezelése vagy azok vonatkozásában nem privát felhőszolgáltatás igénybevétele nem lehetséges, a Hatóság nem hagyja jóvá az EIR használatát.

17 Ennek részleteit lásd a Vhr. V: fejezetében (Sérülékenységvizsgálat).

A másik feladatkör az EIR-ek *biztonsági osztályba sorolása*, amely vizsgálata a Hatóságnak megküldött információk alapján történik. Ha a bejelentett biztonsági osztályba sorolást a Hatóság jóváhagyja, az nem zárja ki a későbbi felülvizsgálat lehetőségét, valamint a Hatóságnak lehetősége van a szervezet által megállapított biztonsági osztályt felülbírálni és indokolással magasabb biztonsági osztályba sorolást is megállapítani vagy alacsonyabb biztonsági osztályba sorolást javasolni. Ha a kiberbiztonsági audit lefolytatása során, a szervezet által megállapított biztonsági osztály megfelelőségének vizsgálata eredményeként az auditor „nem megfelelő" értékelést rögzített, a Hatóság kötelezheti a szervezetet az EIR biztonsági osztályának felülvizsgálatára és módosítására.

Ha a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, vagy nem tartja be, a Hatóság jogkövetkezményeket alkalmazhat. A jogkövetkezmények rendszere – a NIS 2 irányelvben szabályozottakra figyelemmel – az Ibtv.-hez képest többrétűbbé vált: figyelmeztetés, felszólítás, kötelezés, felügyelő szervhez vagy a tulajdonosi joggyakorlóhoz fordulás, információbiztonsági felügyelő kirendelése vagy bírság kiszabása.[18] A Hatóságnak lehetősége van továbbá a magyar kibertér biztonságára fenyegetést jelentő adat ideiglenes hozzáférhetetlenné tételét elrendelni, azonnal végrehajthatónak nyilvánított határozatban, legfeljebb 90 napra (amely további 90 nappal meghosszabbítható), továbbá elektronikus adat ideiglenes eltávolítására kötelezni, amelyre a szervezet a közlését követő 1 munkanapon belül köteles.

A Hatóság a fentieken kívüli további alapvető feladatokat is ellát. Ilyen először is a *hatósági ellenőrzés*, amelyet éves ellenőrzési terv alapján vagy soron kívül végez. Az EIR-ek, és az azokban kezelt adatok biztonsága érdekében jogosult ellenőrizni minden olyan, az EIR védelmére vonatkozó intézkedést, amellyel az érintett EIR-t veszélyeztető fenyegetések kezelhetőek. A Hatóság az ellenőrzés eredményét jegyzőkönyvben rögzíti.

A Hatóság feladata továbbá a *hatósági nyilvántartás* vezetése. Az új EIR fejlesztése esetén a szervezet vezetőjének feladata az adatok, dokumentumok, valamint ezek változásai megküldése a Hatóság részére, a változást követő 14 napon belül, nyilvántartásba vétel céljából, valamint az ellenőrzés lefolytatásához szükséges feltételek biztosítása. A nyilvántartás tartalmazza – többek között – a szervezet EIR-einek megnevezését, rövid leírását, biztonsági osztályának besorolását, a nyilvántartásba vétel, valamint a felülvizsgálat időpontjában elért biztonsági osztály meghatározását, nyilvántartásba vétele dátumát, a nyilvántartás módosításának dátumát; az EIR-ben kezelt adatok osztályozásához kapcsolódó adatokat, azok adatkezelésének helyszínét; az EIR-hez kapcsolódóan igénybe vett felhőszolgáltatásokra vonatkozó adatokat és kapcsolódó védelmi intézkedéseket, azok státuszát; az EIR biztonságáért felelős személy feladatait ellátó személy, szervezet azonosítására alkalmas adatokat; a szervezet információbiztonsági szabályzatát, annak nyilvántartásba vételének dátumát, a nyilvántartás módosításának dátumát; a hatósági ellenőrzésekkel kapcsolatos információkat; valamint a sérülékenységvizsgálat eredményét, valamint a sérülékenységek megszüntetésére vonatkozó sérülékenységkezelési tervet.

18 Ezeket részletesen lásd a Vhr. 37-44. §§ - a Kibertv. 30-32. §§-aiban.

Összegzés

A tanulmányban felvázoltam az elektronikus információs rendszerek fejlesztése folyamatának hatályos eljárásrendjét, kitérve a legfőbb kérdésekre. Ezen új szabályok megalkotása nem várathatott tovább magára, köszönhetően nem csak a NIS 2 implementációs kötelezettségének, hanem annak is, hogy ezek a rendszerek és a mögöttes platformok rohamos gyorsasággal fejlődnek, és megfelelő keretek nélkül félő lenne, hogy az adódó jogi kiskapuk kihasználása nehezen követhető és kontrollálható folyamatokat indítana be. Azért is fontos ezen szabályok ismerete, mert napjainkban alig van az életnek olyan területe, ahol ne találkoznánk ilyen rendszerekkel vagy ne használnánk azt, ezért a biztonságos használat feltételeinek megteremtése az egyik legalapvetőbb elvárás – és ezt szolgálja a fent ismertetett jogszabályi környezet kialakítása is.

FELHASZNÁLT JOGSZABÁLYOK ÉS IRODALOM

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

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információs rendszerei biztonsági osztályba sorolásának és a szervezet biztonsági szintbe sorolásának követelményeiről

187/2015. (VII. 13.) Korm. rendelet az állami és önkormányzati szervek elektronikus információs rendszereinek biztonsági elvárásairól és a logikai védelmi intézkedésekről

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

2013. évi L. törvény az állami és önkormányzati szervek információbiztonságáról (Ibtv.)

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

2024. évi LXIX. törvény Magyarország kiberbiztonságáról

Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2555 Irányelve 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

NKI 2026. *Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója.* Útmutató EIR Fejlesztéséhez.
https://nki.gov.hu/wp-content/uploads/2026/01/NBSZ-NKI-Utmutato_az_elektronikus_informacios_rendszerek_fejlesztesehez-V.1.2.pdf p5