BLACK CELL
Protecting critical infrastructures

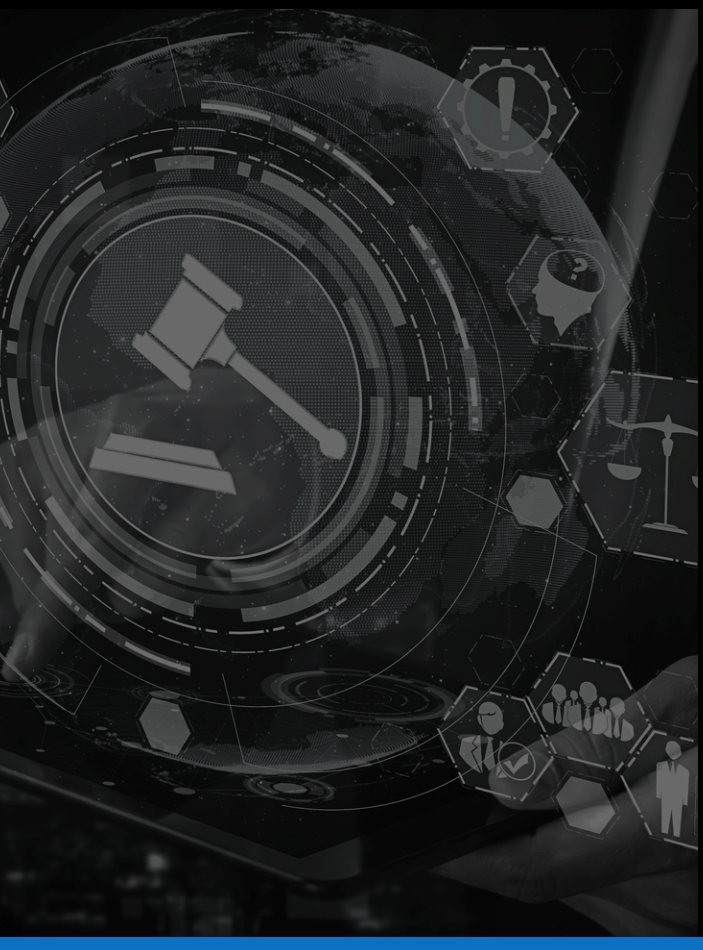
2025 OKTÓBER
FRISSÍTETT VÁLTOZAT

NIS 2 HAZAI IMPLEMENTÁCIÓJA

és a szervezetek előtt álló feladatok

Készítette
dr. Faragó Tamás

Tartalom



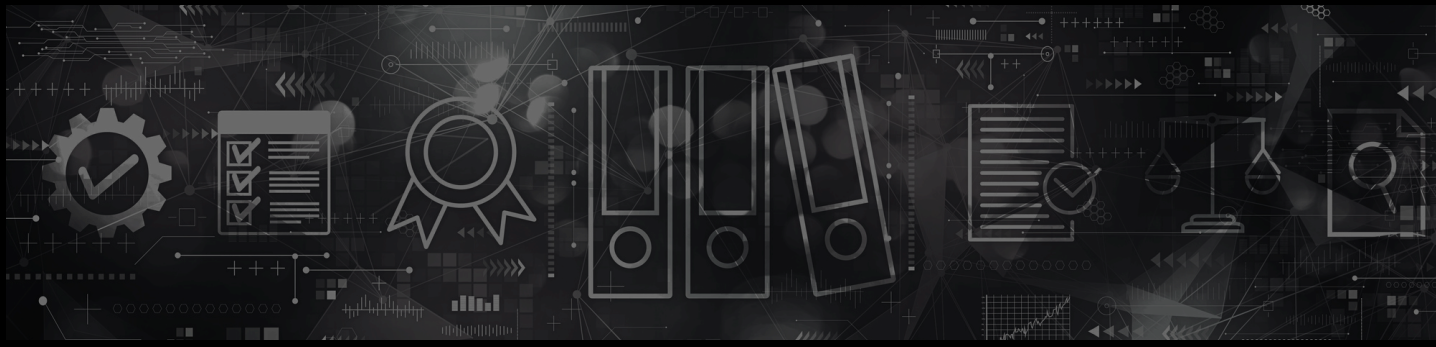
Bevezetés

2022 év végén jelent meg 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 2022/2555. Európai Parmentei és Tanácsi Irányelv (**NIS 2 irányelv**).

A magyar jogalkotó 2023-ban megalkotta a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvényt, valamint a kontrollkövetelményeket tartalmazó a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendeletet. Előbbi azóta hatályát vesztette, helyét pedig 2025. január elsejével átvette a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági törvény) és annak végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet. Azonban ezzel nem oldódott meg az audit kötelezettség kérdése. Ezt oldotta fel a jogalkotó, mikor 2025. január végén, hatályba léptette a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról szóló 1/2025. (I. 31.) SZTFH rendelet, valamint a kiberbiztonsági felügyeleti díjról szóló 2/2025. (I. 31.) SZTFH rendelet.

Hosszas jogalkotói munka után mára teljesen kikristályosodott a teljes rendszer, a jogalkotó rendezte az összes lényeges, szervezeteket érintő kérdést, így a felügyelet módját, a kiberbiztonsági auditok lefolytatására vonatkozó eljárásokat, valamint a befizetendő díjakat, továbbá az eredeti határidőhöz képest a kötelezően lefolytatandó kiberbiztonsági auditok határidejét az eredet 2025. december 31-es határidőről 2026. június 30-ra módosította, esélyt adva szervezeteknek a megfelelőség elérésére, valamint lehetőséget az auditor cégeknek a teljesítésre.

Fontos kiemelni, hogy jelen összefoglaló a **Kiberbiztonsági törvény** 2. és 3. számú melléklete szerinti tevékenységet folytató piaci alapú vállalkozások szemszögéből mutatja be a megfelelőséget.



Vezetői összefoglaló

A szervezetekre vonatkozó legfontosabb kötelezettségek:

A nyilvántartásba vetéli határozat keltétől számított **120 napon belül szerződést kell kötni** az SZTFH **nyilvántartásában** szereplő auditorral.

A **kiberbiztonsági audit legmagasabb díját a SZTFH rendelet határozza meg**, mely függ a szervezet árbevételétől, a biztonsági osztályba sorolt elektronikus információs rendszerek számától és azok biztonsági osztályától. A legalacsonyabb díj nettó 1.750.000 forint.

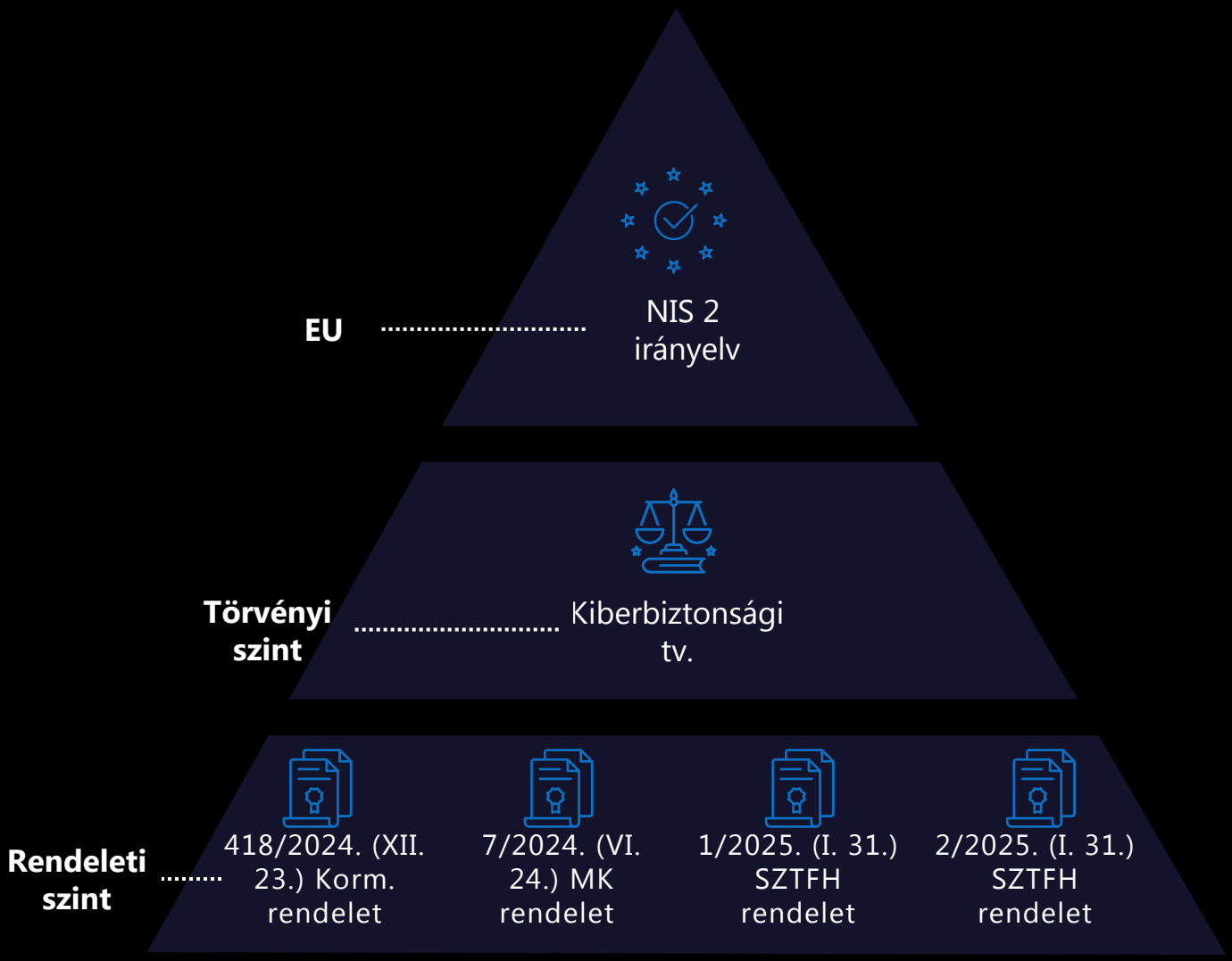
A kiberbiztonsági **audit lefolytatásának rendjét SZTFH rendelet határozza meg**. Az auditor vizsgálhatja a dokumentumok mellett a szervezet által üzemeltetett információs rendszereket, illetve interjúkat is lefolytathat.

A kiberbiztonsági auditon **vizsgálatra kerülnek** az üzemeltett elektronikus **információs rendszerek**, valamint a **szervezet maga** is. Mind a két terület egy-egy megfelelőségi értéket kap egy képlet alapján védelmi megfelelési index (VMI), illetve szervezet ellenálló-képességi indexét (SZEKI). A fentiek közül **bármelyik érték 70 (%) alatti, a szervezet az auditon nem felel meg**.

A hatóság részére fizetendő kiberbiztonsági felügyeleti díjat 2024. évre is meg kellett fizetni időarányosan (2024.10.18.-2024.12.31.) együttesen a 2025. évi díjjal, melyről a határozatot a szervezetek jelen whitepaper megjelenéséig mind megkapták. A díj mértékének felső határa függ a szervezet nettó árbevételétől. A hatóság a felügyeleti díj mértékéről a szervezeteket 2025. május 31-ig tájékoztatta. A befizetés határideje 2025. július 31. volt.

A **kiberbiztonsági bírság** tételes meghatározása – hasonlóan a GDPR-ban megismert rendszerhez – a **szervezet éves nettó árbevételétől függő** 10, illetve 7 millió euró, illetve ha a nettó árbevétel ennél magasabb, úgy 2%, illetve 1,4% is lehet. Emellett persze vannak **olyan bírságtételek**, ahol a jogalkotó **minimum és maximum összegeket határozott meg** (500.000 és 150.000.000 forint között).

Szabályozási keretrendszer



Európai Unió joga

A 2024. október 18-án alkalmazási hatályba lépett **NIS 2 irányelv** a 2016-ban kiadott NIS irányelvet váltotta, jóval részletesebb szabályokkal, szélesebb kötelezetti körrel.
Ez számtalan cég életében hozott kisebb-nagyobb változást, hiszen voltak olyan szervezetek, melyek korábban is a NIS irányelv hatálya alá tartoztak, azonban számtalan olyan szervezet is a hatálya alá került, amelyek korábban nem voltak ilyen jellegű kötelezettség címzettjei.

A NIS 2, irányelv jellege miatt megkövetelte a tagállamoktól, hogy az abban foglaltakat ültessék át a nemzeti jogrendjükbe (implementálás).

Magyarországi implementáció

Törvényi szint

A hazai szabályozás kétszintű, vagyis a jogalkotó törvényi szinten rögzíti a magas szintű elvárásokat, ezt követően rendeleti szinten írja elő a részletszabályokat. A szabályozás megtartja a korábbi dichotóm rendszert, leegyszerűsítve a közigazgatási és állami hátterű szervezetek hatóságaként a nemzeti kiberbiztonsági hatóságot jelöli ki, míg a piaci szereplők esetén az SZTFH-t jelöli ki hatóságként.

2023-ban a **NIS 2 irányelv** hazai implementációjára megszületett a már hatályát veszett, a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (**Kibertan.tv.**). Itt kerültek lefektetésre az alapelvek, a magas szintű szabályok.

2024. év végén jelent meg a Magyar Közlönyben, valamint 2025. január 1-jén vált hatályosság a **Magyarország kiberbiztonságáról szóló 2024. LXIX. törvény** (**Kiberbiztonsági tv.**), mely az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.), valamint az alig egy évet megélt Kibertan.tv. helyébe lépett, kvázi „összegyúrva" azt egyetlen, a hazai kiberbiztonságot szabályozó normává.

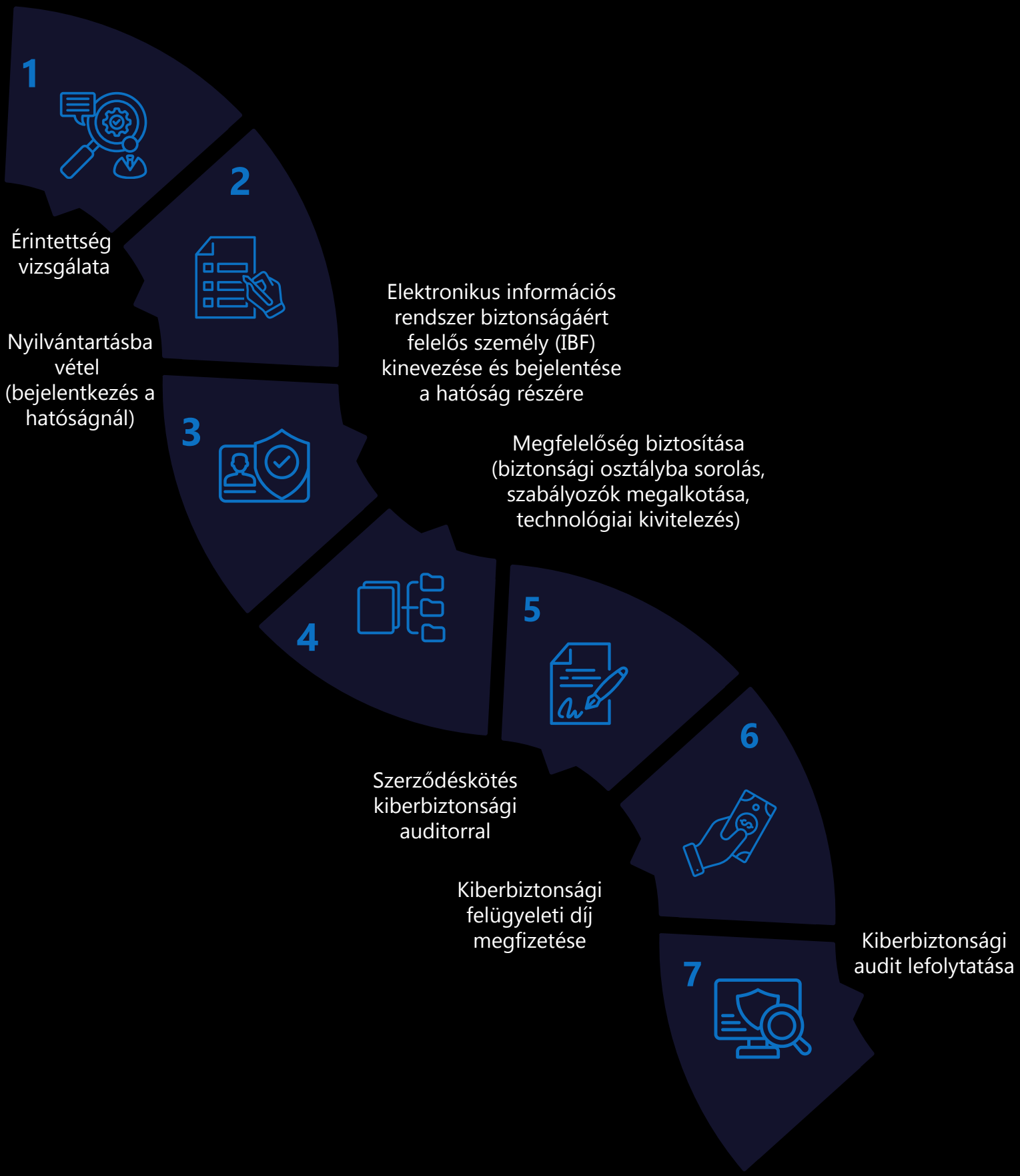
Rendeleti szint, a részletszabályok

Szintén 2024. év végén hirdette ki a jogalkotó a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló **418/2024. (XII. 23.) Korm. rendelet** (**Korm. rendelet**), mely a **Kiberbiztonsági tv.** végrehajtásával kapcsolatos részletszabályokat tartalmazza. A végrehajtás módja mellett meghatároz számos hatósági feladatot, illetve pontosítja a kiszabható bírások körét és nagyságát.

Az alsóbb rendű szabályozók második nagy szelete a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (**MK rendelet**), mely a konkrét, szervezetektől elvárt védelmi intézkedéseket (kontrollkövetelményeket) tartalmazta. A normaszöveg a NIST 800-53 rev. 5-re alapul. A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete** egy – azóta már frissített – útmutatót is közzétett, mely egyrészt megkönnyíti a szervezeteknek az egyes védelmi intézkedések alkalmazását, másrészt, amennyiben a szervezet a korábban hatályos **41/2015. (VII. 15.) BM rendelet** szerint alakította ki az információbiztonsági irányítási keretrendszerét, esetleg ISO 27001:2022 alapon tette mindezt, úgy meg tudja feleltetni az egyes kontrollokat az új normában rögzítettekkel.

Végül **megjelent** a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról szóló **1/2025. (I. 31.) SZTFH rendelet**, mely rendezi a kiberbiztonsági audit lefolytatásának egységes módszertanát, a szervezetektől elvártakat, valamint a kiberbiztonsági audit maximális díját, megjelent a kiberbiztonsági felügyeleti díjról szóló **2/2025. (I. 31.) SZTFH rendelet**, mely rendezi a kiberbiztonsági felügyeleti díj mértékét, megfizetésének módját.

Szervezeti feladatok



1 Érintettség vizsgálata

Minden szervezetnek az **első lépés, hogy megvizsgálja, érintett-e**, tehát vonatkozik-e rá a jogszabály. Amennyiben nem, úgy természetesen nincsen teendője.

Amennyiben viszont a **Kiberbiztonsági tv.** hatálya alá tartozik a szervezet, úgy köteles bizonyos feladatok elvégzésére, valamint – szervezet ágazati hovatartozásától függően – bizonyos díjak megfizetésére.

Az érintettség vizsgálatához két dologra van szükség:

- a szervezet valós, valamint a közhiteles cégnyilvántartásban is rögzített tevékenységeinek áttekintésére, valamint összevetésére a **Kiberbiztonsági tv.** 2. és 3. sz. mellékletével, illetve
- Bizonyos esetektől eltekintve a **Kiberbiztonsági tv.** csak a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvény (**Kkvtv.**) szerinti egyes vállalatokra vonatkozik. Így tehát – egyes kivételektől eltekintve nem vonatkozik a mikro- és kiválallkozásokra.

A kivételek, melyek méretüktől függetlenül a Kiberbiztonsági tv. hatálya alá tartoznak:

- elektronikus hírközlési szolgáltató,
- bizalmi szolgáltató,
- DNS-szolgáltató,
- legfelső szintű doménnév-nyilvántartó vagy
- doménnév-regisztrációt végző szolgáltató.

A **Kiberbiztonsági tv.** hatálya kiterjed **a közigazgatási szervekre, a többségi állami befolyás alatt álló gazdálkodó szervezetekre**, amennyiben megfelelnek a **Kkvtv**. szerinti feltételeknek (50 fős foglalkoztatotti létszám vagy bevételi/mérlegfőösszeg adatok), a **honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságokra**, valamint a kritikus szervezetek ellenálló képességéről szóló törvény (**Kszetv**.) alapján kijelölt **kritikus szervezetekre**, továbbá a védelmi és biztonsági tevékenységek összehangolásáról szóló törvény (Vbö.) alapján kijelölt, az **ország védelme és biztonsága szempontjából jelentős szervezetek** és infrastruktúrák üzemeltetőire.

Amennyiben a szervezetek a **Kiberbiztonsági tv.** 2. és 3. sz. mellékletében foglalt tevékenységet végzik, továbbá – a fenti eseteket ide nem értve – nem minősülnek mikro- és kiválallatnak, úgy a törvény hatálya alá tartoznak és minden a továbbiakban felsorolt kötelezettség címzettjei.

Mikro- illetve kisvállalati érintettség esetén két dolgot kell vizsgálnia a szervezeteknek:

- foglalkoztatotti létszámadatot,
- éves nettó árbevételt vagy mérlegfőösszeget.

2 Nyilvántartásba vétel (bejelentkezés a hatóságnál)

Azon szervezeteknek, akik a tevékenységüket 2024. január 1. napja előtt kezdték meg, 2024. június 30-ig voltak kötelesek bejelentkezni a felügyeleti hatóságnál (Szabályozott Tevékenységek Felügyeleti Hatósága - SZTFH).

Amely szervezet a **nyilvántartásba vételt elmulasztotta, vagy a jövőben elmulasztja** az a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet (**Korm. rendelet**) 3. sz. melléklete értelmében komoly **bírságtételre számíthat** (minimum bírságtétel: előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának 0,5%-a, de legalább 1 000 000 forint, maximum bírságtétel: előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának legfeljebb 2%-a, de legfeljebb 150 000 000 forint).

Az a szervezet, amely a **Kiberbiztonsági tv.** hatálya alá tartozást megalapozó **tevékenységét később kezdi meg vagy a középvállalkozás méretet később éri el**, köteles az adatokat az érintett hatóság részére **30 napon belül** megküldeni.

3 Elektronikus információs rendszer biztonságáért felelős személy (IBF) kinevezése és bejelentése a hatóság részére

A szervezet, mely a **Kiberbiztonsági tv.** hatálya alá tartozik köteles **elektronikus információs rendszerek biztonságáért felelős személy (IBF) kinevezésére**, valamint adatainak megküldésére az illetékes hatóság részére **30 napon belül**.

Az IBF **lehet a szervezet alkalmazottja, de akár külsős vállalkozó** által, megbízás keretében biztosított személy is. Amennyiben a szervezetek külsős vállalkozót bíznak meg az IBF szerepkör ellátásával, úgy a vonatkozó szerződés tartalmi elemeire a jogalkotó bizonyos követelményeket előír. Emellett alapvető szervezeteknél legalább kéthavonta egy napon, fontos szervezeteknél legalább háromhavonta egy napon – dokumentált módon – az érintett szervezetnél való fizikai jelenlét mellett köteles ellátni.

Bizonyos esetekben (kritikus szervezetek, az ország védelme és biztonsága szempontjából jelentős szervezetek, közigazgatási szervezetek) az **IBF-nek rendelkeznie kell** szaktudását biztosító, a jogalkotó által előírt **képesítéssel** vagy nemzetközi képzettséggel, továbbá meghatározott szakmai tapasztalattal. Az elfogadható **végzettségek listáját** az NBSZ NKI **honlapján** teszi közzé.

4 Megfelelőség biztosítása (biztonsági osztályba sorolás, szabályozók megalkotása, technológiai kivitelezés)

A szervezetek feladatai természetesen nem állnak meg a nyilvántartásba vétel, valamint az IBF kijelölésével; az **elektronikus információs rendszereiket fel kell mérniük, valamint azok közül azokat, melyek rendelkezésükben állnak, biztonsági osztályba kell sorolniuk** (alap, jelentős, magas). A biztonsági osztályba sorolása eredményeképpen láthatóvá válik, hogy az **MK rendelet** védelmi intézkedései közül melyeket kell alkalmazniuk.

Emellett a szervezeti és információs rendszert érintő **kockázataikat fel kell mérniük** legalább a 7/2024. (VI. 24.) MK rendelet 3. számú melléklete szerinti tartalommal. A kockázatok figyelembevételével meg tudják határozni, hogy az egyes bevezetendő kontrollokat alkalmazzák, esetleg kizárják az alkalmazhatóságukat, vagy eltéréssel alkalmazzák azokat. Amennyiben egy **védelmi intézkedést a szervezetek nem tudnak vagy nem kívánnak alkalmazni**, esetleg **eltéréssel kívánnak alkalmazni, úgy azokat minden esetben meg kell indokolniuk**. Ehhez ki kell tölteniük a 1/2025. (I. 31.) SZTFH rendelet 4. sz. melléklete szerinti **eltérések és helyettesítő védelmi intézkedések nyilvántartását**, melynek átadása az auditor számára nélkülözhetetlen.

A szervezeteknek a megfeleléshez tehát legalább az alábbiakat kell elvégezniük:

- elektronikus információs rendszerek felmérése,
- a rendelkezésükben álló rendszerek biztonsági osztályba sorolása,
- az eltérések és helyettesítő védelmi intézkedések listájának kitöltése,
- szabályozókat kell alkotniuk és azokat folyamatosan felül kell azokat vizsgálniuk,
- információbiztonsági irányítási rendszert kell működtetniük és erről auditálható bizonyítékokat kell gyűjteniük (pl. jegyzőkönyvek, jelenléti ívek, etc.),
- terveket kell alkotniuk és tesztelniük (pl. incidenskezelési terv, üzletmenet-folytonossági tervek, karbantartási terv, etc.),
- a kockázataikat folyamatosan monitorozniuk kell,
- megfelelő fizikai és környezeti biztonságot kell teremteniük összhangban az információs rendszer biztonsági osztályában elvárt követelményekkel,
- be kell vezetniük az elvárt és kockázatokkal arányos technikai védelmi intézkedéseket (pl. tűzfal, MDM, etc.)

5 Szerződéskötés kiberbiztonsági auditorral

A szervezeteknek, akiket a hatóság nyilvántartásba vett, kötelesek egy, a kiberbiztonsági audit lefolytatására jogosult, az SZTFH **nyilvántartásában** szereplő auditorral szerződést kötni a **2 évente kötelező kiberbiztonsági audit** elvégzése érdekében.

A **szerződést** a szervezeteknek a **nyilvántartásba vételt követő 120 napon belül** kell megkötniük. A kiberbiztonsági auditor az **auditot díjazás ellenében végzi**, melynek felső határát a jogalkotó meghatározta.

6 Kiberbiztonsági felügyeleti díj megfizetése

A **szervezeteknek évente kiberbiztonsági felügyeleti díjat kell fizetniük az SZTFH részére**. A kiberbiztonsági felügyeleti díj **felső határát a jogalkotó meghatározta**; szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – legfeljebb 0,015 százaléka, de legfeljebb 10 millió forint.

Az ugyanazon elismert vállalatcsoportban vagy az ugyanazon, a Polgári Törvénykönyvről szóló törvény szerinti tényleges vállalatcsoportban, vagy a számvitelről szóló törvény szerinti anyavállalatot, leányvállalatokat és a konszolidálásba bevont közös vezetésű vállalkozásokat tartalmazó, egy konszolidációs körbe tartozó vállalkozáscsoportban részt vevő szervezetek tekintetében a fizetendő éves kiberbiztonsági felügyeleti díj együttes mértéke nem haladhatja meg az 50 millió forintot. A tényleges vállalatcsoportként vagy az egy konszolidációs körbe tartozó vállalkozáscsoportként való működés tényét az (1) bekezdés szerinti szervezet az SZTFH elnökének rendeletében foglaltak szerint igazolja.

7 Kiberbiztonsági audit lefolytatása

A kiberbiztonsági auditot a szervezettel szerződéses kapcsolatban álló kiberbiztonsági auditor végzi el. A kiberbiztosági **audit módszertanát a jogalkotó határozta meg** annak érdekében, hogy egységes és objektív tudjon lenni.
Az audit módszertan a NIST Special Publication 800-53A Revision 5 dokumentum alapján került kialakításra.

A **vizsgálatok célja** annak megállapítása és bizonyítékokkal történő alátámasztása, hogy az MK rendelet szerint **bevezetett intézkedések tartalmaznak-e hibákat vagy hiányosságokat**, illetve, hogy azok megfelelően működnek-e.

A vizsgálatok lefolytatásának módszerei:
- dokumentumvizsgálat,
- interjú,
- teszt.

Az egyes kontrollcsoportok esetén az auditor a fenti módszereket alkalmazva az alábbi megállapításokat teheti:
- nem alkalmazható (NA), ha az alkalmazhatóságot a szervezet kizárta vagy eltéréssel alkalmazza a kontrollt, amennyiben az auditor ezzel egyetért, vagy az értékelésből az auditor a követelménycsoportot kizárta,
- nem megfelelt (NM), amennyiben követelmény teljesülésére nincs bizonyíték vagy a szervezet nem vállalja az intézkedés megvalósítását,
- megfelelt (M), amennyiben a kötelező vizsgálati módszerek alapján az elemi követelmény teljesülésére vonatkozó bizonyítékok rendelkezésre állnak.

A dokumentumvizsgálat kiterjedhet:
- belső szabályozók (stratégiák, politikák, IBSZ, eljárásrendek) vizsgálatára,
- rendszerleírások vizsgálatára,
- jegyzőkönyvekre, jelenléti ívekre, ellenőrzési és egyéb tervekre.

Az interjúk megvalósulhatnak a folyamatok tisztázása érdekében:
- írásbeli interjúkérdésekkel,
- szóbeli interjúkérdések formájában.

Az interjúk lehetnek helyszíniek vagy elektronikus hírközlő eszköz igénybevételével távoli interjúk, melyeket az auditor az IBF jelenlétében végez.

A tesztek kiterjedhetnek
- automatizált ellenőrző programokkal, vagy – a szervezet munkatársainak közreműködésével végrehajtott – céltesztek

Az auditálási eljárás kiterjed:
- elektronikus információs rendszerek besorolása megfelelőségének és vezető általi jóváhagyásának ellenőrzésére,
- egyes követelménycsoport szervezeti vagy elektronikus információs rendszerre vonatkozó megfelelőségére.

A követelménycsoportok vizsgálata során az auditor:
- megfelelt, minősítést ad, ha az elemi követelmények mindegyike „megfelelt" vagy „nem alkalmazható" értékelést kapott,
- ha a vizsgált követelménycsoportra van egy vagy több olyan elemi követelmény, amelyre vonatkozóan az auditor „nem megfelelt" döntést hozott, akkor az auditor az eltérést minősíti. A minősítés során az auditor különösen a következő szempontokat veszi figyelembe:
  - a „nem megfelelt" döntések száma,
  - az auditornak a komplex rendszerre, más intézkedésekre vonatkozó ismeretei, figyelembe véve a nem megfelelőségek támadó oldali kihasználási lehetőségeit

A minősítés során az auditor különösen a következő szempontokat veszi figyelembe:
- a „nem megfelelt" döntések száma,
- az auditornak a komplex rendszerre, más intézkedésekre vonatkozó ismeretei, figyelembe véve a nem megfelelőségek támadó oldali kihasználási lehetőségeit.

Az eltérés minősítése lehet:

Eltérés mértéke	Leírás	Pont levonás
kis mértékű eltérés	a vonatkozó biztonsági elvárások kisebb hiányosságokkal, de alapvetően céljuknak megfelelően működnek	4
kiemelt mértékű eltérés	az elvárt intézkedés fő céljai nem teljesülnek	10
kritikus mértékű eltérés	az intézkedés nem megfelelése olyan súlyú, hogy személyi sérülés, személyes adatok bizalmasságának sérülése, nemzeti adatvagyon sérülése, létfontosságú rendszer rendelkezésre állásának sérülése, a szervezet üzlet- vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer, vagy információt képező adat sérülése bekövetkezési valószínűségét növeli	10000

Az egyes követelménycsoportokat az auditor megfelelőségük szerint pontértékkel látja el:

- megfelelt esetén 0,
- elhanyagolható mértékű eltérés esetén 1,
- kis mértékű eltérés esetén 4,
- kiemelt mértékű eltérés esetén 10
- kritikus mértékű eltérés esetén 1000

A fenti értékek segítenek kiszámolni a védelmi megfelelési indexet (VMI).

A VMI megfelelőségi értékelése:

Eltérés mértéke	Az EIR-nek a védelmi intézkedések katalógusa elvárásainak való megfelelés szempontjából történő értékelése
VMI ≥ 95	Megfelel
90 ≤ VMI < 95	Alacsony kockázattal megfelel
80 ≤ VMI < 90	Jelentős kockázattal megfelel
70 ≤ VMI < 80	Magas kockázattal megfelel
VMI < 70	Nem felel meg

Az auditor köteles a szervezetet is értékelni. Ekkor azon követelménycsoportokat veszi figyelembe melyek nem elektronikus információs rendszer, hanem szervezeti szinten értékelhetőek.

Az auditor meghatározza – hasonlóan a VMI indexhez – a szervezet ellenálló-képességi indexét (SZEKI):

Szervezet értékelése	A szervezetnek a védelmi intézkedések katalógusa elvárásainak való megfelelés szempontjából történő minősítése	Értékelés eredménye
SZEKI ≥ 95	Elhanyagolható kockázattal megfelel	Megfelelt
90 ≤ SZEKI < 95	Alacsony kockázattal megfelel	Auditált
80 ≤ SZEKI < 90	Jelentős kockázattal megfelel	
70 ≤ SZEKI < 80	Magas kockázattal megfelel	
SZEKI < 70	Kritikus kockázattal nem felel meg	Nem megfelelt

Az audit során az alábbiak mentén kerülnek vizsgálatra a rendszerek:

Biztonsági osztály	Vizsgálandó rendszerek (százalék)
Alap	Ki kell terjednie a szervezet információs rendszereinek **legalább 40%-ára**, de ha van, **legalább egy** alap **rendszerre**.
Jelentős	Ki kell terjednie a szervezet információs rendszereinek **legalább 60%-ára**, de ha van, **legalább egy** alap **rendszerre**.
Magas	Ki kell terjednie a szervezet információs rendszereinek **legalább 70%-ára**, de ha van, **legalább egy** alap **rendszerre**.

Díjak

Kiberbiztonsági felügyeleti díj

A kiberbiztonsági felügyeleti díjat a szervezeteknek évente kell megfizetniük a Magyar Államkincstár által vezetett, 10032000-00362887-00000000 számú előirányzat-felhasználási keretszámlájra átutalással. A közlemény rovatában fel kell tüntetni a „kiberbiztonsági felügyeleti díj" megjegyzést és:

- SZTFH felügyeleti díj mértékéről szóló tájékoztatás iktatószámát,
- Nyilvántartásba vételi határozat iktatószámát vagy a törlési határozat iktatószámát, amennyiben a tárgyévben került a **Kiberbiztonsági tv.** hatálya alá a szervezet vagy tárgyévben került ki a hatálya alól.

A díj mértéke szervezet tárgyévet megelőző évben közzétett utolsó, a számvitelről szóló 2000. évi C. törvény (**Szt.**) szerinti beszámolója szerinti **nettó árbevételének 0,00015 százaléka**, ha a szervezet tárgyévet megelőző **éves nettó árbevétele nem éri el a 20 milliárd forintot**.

A díj mértéke a szervezet tárgyévet megelőző évben közzétett utolsó, **Szt.** szerinti beszámolója szerinti nettó árbevételének **0,0015 százaléka, de legfeljebb 10millió forint**, ha a szervezet tárgyévet megelőző **éves nettó árbevétele eléri vagy meghaladja a 20 milliárd forintot.**

Díj mértéke (nettó árbevétel %-os aránya)	éves nettó árbevétele nem éri el a 20 milliárd forintot	éves nettó árbevétele eléri vagy meghaladja a 20 milliárd forintot
	nettó árbevételének 0,00015 százaléka	nettó árbevételének 0,0015 százaléka

Maximuma 10 millió forint, vállalatcsoport esetén 50 millió forint.

Az elszámolás 1000 forintos kerekítés szerint történik, az általános kerekítési szabályok szerint.

Amennyiben a szervezet év közben kerül a **Kiberbiztonsági tv.** hatálya alá, úgy időarányos mértékű díjfizetésre kötelezett. Évközbeni törlés esetén a törlés napjáig fennálló időarányos összeg fizetendő.

Ha a tárgyévben fizetendő kiberbiztonsági felügyeleti díj összege nem éri el az 5000 forintot, a kiberbiztonsági felügyeleti díjat nem kell megfizetni.

A szervezet a **Ptk.** szerinti elismert vállalatcsoportban, tényleges vállalatcsoportban vagy az **Szt.** szerinti anyavállalatot, leányvállalatokat és a konszolidálásba bevont közös vezetésű vállalkozásokat tartalmazó, egy konszolidációs körbe tartozó vállalkozáscsoportban vesz részt, a szervezet a részvételét a Hatóság által e célra rendszeresített elektronikus űrlapon benyújtott – elismert vállalatcsoport esetében az uralkodó taggal közösen megtett – nyilatkozatával igazolja a Hatóság részére a tárgyév január 31. napjáig (igazolás). Ebben nyilatkozik a tárgyévi árbevétele egész évre vetített időarányos részének összegéről a tárgyév február 28. napjáig.

A hatóság a felügyeleti díj mértékéről és megfizetés módjáról a tárgyév március 31. napjáig tájékoztatja a szervezeteket.

Ha a szervezetek vállalatcsoport tagjaként működnek és a kiszabott díj meghaladná az 50 millió forintot, úgy szervezetek tárgyév április 30-ig közös nyilatkozatot nyújtanak be a Hatóság részére, amely tartalmazza az egyes szervezetek által megfizetésre kerülő kiberbiztonsági felügyeleti díj összegét, azzal, hogy a megfizetésre kerülő kiberbiztonsági felügyeleti díj együttes mértéke összesen 50 millió forint.

A kiberbiztonsági felügyeleti díjat a tárgyév május 31. napjáig kell megfizetni.

A 2024 évi kiberbiztonsági felügyeleti díj mértékének megállapításakor a hatóság a szervezet 2024. évet megelőző utolsó, Szt. alapján közzétett beszámolóval lezárt üzleti évről szóló beszámolója alapján állapítja meg. A 2024. évre vonatkozó kiberbiztonsági felügyeleti díjat a 2024. október 18-tól 2024. december 31-ig terjedő felügyeleti időszakra kellett megfizetni.

2025 évre vonatkozóan:

- a vállalatcsoporti nyilatkozatot 2025. március 15. napjáig kellett megküldenie a szervezeteknek a hatóság részére,
- amennyiben a tagvállalatok által fizetendő felügyeleti díj mértéke az 50 millió forintot meghaladná, az erről szóló nyilatkozatot 2025. június 30. napjáig kellett benyújtania szervezeteknek a hatóság részére.
-

A 2024. és 2025 évekre fizetendő kiberbiztonsági felügyeleti díjról szóló tájékoztatást a hatóság 2025. május 31-ig megtette.

A 2024. és 2025 évekre fizetendő kiberbiztonsági felügyeleti díjat 2025. július 31-ig kellett megfizetnie a szervezeteknek.

Kiberbiztonsági audittal összefüggő díjazás

A kiberbiztonsági auditok díját SZTFH rendelet határozza meg. A jogalkotó a kiberbiztonsági audit díjának felső korlátját adta meg az 1/2025. (I. 31.) **SZTFH rendelet** 3. sz. mellékletében.

A kiberbiztonsági audit díjának maximuma több dologtól függ, köztük:
- szervezet előző évi nettó árbevétele,
- besorolt elektronikus információs rendszerek száma,
- besorolt elektronikus információs rendszerek biztonsági osztálya

A kiberbiztonsági audit díj-maximuma a fenti faktorokhoz tartozó szorzószámok az alapdíjjal, vagyis a nettó 1.750.000 forinttal való megszorzásának eredménye.

Árbevétel	
A szervezet előző üzleti évi nettó árbevétele	**Szorzószám**
árbevétel ≤ 1 milliárd Ft	0,9
1 milliárd Ft < árbevétel ≤ 5 milliárd Ft	1,1
5 milliárd Ft < árbevétel ≤ 10 milliárd Ft	1,9
10 milliárd Ft < árbevétel ≤ 15 milliárd Ft	2,5
15 milliárd Ft < árbevétel ≤ 25 milliárd Ft	2,75
25 milliárd Ft < árbevétel ≤ 40 milliárd Ft	3
árbevétel > 40 milliárd Ft	4

Elektronikus információs rendszerek száma	
Elektronikus információs rendszerek száma	**Szorzószám**
1-5	1
6-15	2,5
16 vagy annál több	4

Biztonsági osztály besorolása	
Biztonsági osztály	**Szorzószám**
alap	1
jelentős	3
magas	5

A ténylegesen fizetendő **díjat az auditor cég állapítja meg** (ajánlatot tesz, melyet a szervezet elfogadhat vagy elutasíthat).

A fizetendő díj maximuma tehát az alábbiak szerint alakul:

Nettó 1.750.000 Ft **X** Árbevétel szerinti szorzószám **X** Elektronikus információs rendszerek szerinti szorzószám **X** Biztonsági osztály szerinti szorzószám

Bírságok

A kiberbiztonsági hiányosságokkal kapcsolatos korábbi bírságtételek nem feltétlenül hozták meg a várt hatást, hiszen elrettentő erejük nem igazán volt. A **Kiberbiztonsági tv.** és **végrehajtási rendelete** (3. sz melléklet) azonban **sokkal magasabb bírságtételekkel operál**.

Amikor bírságokról beszélünk mindenképpen ki kell emelni, hogy a hatóságok a fokozatosság elvét alkalmazzák, továbbá figyelembe veszik a **súlyosbító és enyhítő körülményeket**, melyeket a **3/2025. (IV. 17.) SZTFH rendelet** 6. §-a tartalmaz.

A szabálytalanság megnevezése	A bírság legkisebb mértéke	A bírság legnagyobb mértéke
A nyilvántartásba vétel érdekében történő adatszolgáltatás nem teljesítése	szervezet előző üzleti évi **nettó árbevételének** – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának **0,5%-a**, **de legalább 1 000 000 forint**	szervezet előző üzleti évi **nettó árbevételének** – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának **legfeljebb 2%-a, de legfeljebb 150 000 000 forint**
A nyilvántartásba vétel érdekében történő adatszolgáltatás határidőn túl történő teljesítése	**50 000 forint**	szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – vagy előző évi költségvetési bevételi előirányzatának **legfeljebb 0,1%-a, de legfeljebb 15 000 000 forint**
A felügyeleti díjfizetés elmulasztása	**500 000 forint**	a kiberbiztonsági **éves felügyeleti díj maximum tízszerese**
Adatváltozás megküldésének elmulasztása	**50 000 forint**	**1 000 000 forint**
Kockázatmenedzsment keretrendszer működtetésének nem teljesítése	**1 000 000 forint**	**Alapvető szervezet** (2. sz. melléklet) esetén **10 millió euró vagy** a ez magasabb a szervezet előző pénzügyi **évi globális éves forgalma teljes összege 2%-ának** megfelelő összeg. **Fontos szervezet** (3. sz. melléklet) esetén **7 millió euró vagy** a ez magasabb a szervezet előző pénzügyi **évi globális éves forgalma teljes összege 1,4%-ának** megfelelő összeg

A szabálytalanság megnevezése	A bírság legkisebb mértéke	A bírság legnagyobb mértéke
A nyilvántartásban szereplő auditorral a kiberbiztonsági audit elvégzésére irányuló megállapodás határidőben történő megkötésére vonatkozó kötelezettség teljesítésének elmulasztása	**1 000 000 forint**	**15 000 000 forint**
A kiberbiztonsági audit határidőn belüli lefolytatásának elmulasztása	**1 000 000 forint**	a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet előző üzleti **évi nettó árbevételének** – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – vagy előző évi költségvetési bevételi előirányzatának **legfeljebb 2%-a, de legfeljebb**
		150 000 000 forint
A kiberbiztonsági incidensek bejelentési kötelezettségének elmulasztása	**500 000 forint**	**5 000 000 forint**

A kiberbiztonsági auditok a gyakorlatban

Kiberbiztonsági audit díja

Az **alap biztonsági osztályba sorolt** rendszerekkel bíró szervezetek esetén – tapasztalataink szerint – a kiberbiztonsági auditok díjazására vonatkozó képlet szerint kiszámolt **maximális díjhoz közeli ajánlatokat adnak az auditorok**, tehát érdemes ezzel számolnia a szervezeteknek.
A **jelentős vagy magas biztonsági osztályba sorolt** rendszerekkel bíró szervezetek esetén – tapasztalataink szerint – a kiberbiztonsági auditok díjazására vonatkozó képlet szerint kiszámolt **maximális díjból 10-20 %-ot is engednek az auditor cégek**.

Kiberbiztonsági audit

A jogszabályváltoztatások lehetővé tették a szervezeteknek, hogy a korábban 2025. december 31-ei határidő helyett, **2026. június 30. napjáig** végeztessék el a kiberbiztonsági auditokat.

A kiberbiztonsági auditokat lefolytató **szervezetek többsége** olyan, a szervezet vagy akár a szervezet által megbízott külső partner által is használható **weboldalakat hoztak létre**, mely felületeken az auditevidenciák feltölthetőek, illetve az audit kérdőívek kitölthetőek. Természetesen akadnak olyan auditorok is, akik ilyen lehetőséget nem kínálnak a szervezeteknek.

Az auditevidenciákat és a kérdőíveket a szervezeteknek a vonatkozó **1/2025. (I.31) SZTFH rendelet** **7. számú módszertani mellékelte szerinti részletességgel kell kitölteniük**, mely nagy körültekintést és sok időt vesz igénybe, ezért ajánljuk a szervezeteknek, hogy erre a hagyjanak időt maguknak, ez akár 1 hónapot is igénybe vehet, függően az információs rendszerek számosságától és az evidenciák mennyiségétől.

Mi a teendőnk, ha szervezetünk a jogszabályok hatálybalépése után kerül azok hatálya alá?

A feladatok a fentiektől nem térnek el, egyedül a határidőkben tapasztalhatunk változást. A jogszabály hatálya alá kerülés tekintetében az alábbi napok irányadóak:

- **Újonnan létesült szervezet** esetén a cégbejegyzés (létesítés) napja,
- **Új**, a hatálybalépést megalapozó **tevékenység** (2. és 3. melléklet szerinti tevékenység) megkezdése esetén a **tevékenység megkezdésének**, vagy cégbejegyzésének **napja**,
- **Kkvtv.**-ből eredő **méretkorlát** (50 fő vagy 10 millió nettó árbevétel vagy mérlegfőösszeg) **átlépése** esetén a **következő év első napja**

A határidők:

- A fenti naptól számított **30 napon belül** megküldi a **bejelentéshez** szükséges adatokat a hatóság részére,
- A nyilvántartásba vételt követő **120 napon belül szerződést köt** a kiberbiztonsági **auditorral**,
- A nyilvántartásba vételt követő **2 éven belül elvégezteti** a kiberbiztonsági **auditot**

A Black Cell Magyarország Kft. szolgáltatásai

Szolgáltatás	Üzletág
Az MK rendelet és a Kiberbiztonsági tv. által elvárt védelmi intézkedések megfelelőség-vizsgálata a szervezet jelenlegi érettségi szintjének megállapítása (gap assessment)	Compliance
Biztonsági osztályba sorolás és szükséges adminisztratív, fizikai, logikai védelmi intézkedések tervezése és bevezetése	Compliance
Szükséges és hiányzó logikai (technikai) védelmi megoldások bevezetése (pl. monitoring, tűzfal, SIEM, SOC, stb.)	Integration / Fusion Center
Rendszeres és szerepköralapú tudatosítás (e-learning)	Black Cell Academy
Sérülékenységvizsgálat, social engineering szimuláció	Offensive security

Felhasznált jogszabályok

- 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 2022/2555. Európai Parmentei és Tanácsi Irányelv (**NIS 2 irányelv**),
- a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (**Kibertan.tv.**),
- Magyarország kiberbiztonságáról szóló 2024. LXIX. Törvény (**Kiberbiztonsági tv.**)
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (**Ibtv.**)
- a kritikus szervezetek ellenálló képességéről szóló törvény (**Kszetv.**)
- a védelmi és biztonsági tevékenységek összehangolásáról szóló törvény (**Vbö**.)
- a számvitelről szóló 2000. évi C. törvény (**Szt.**)
- a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvény (**Kkvtv.**)
- a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (**MK rendelet**),
- Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet (**Korm. rendelet**)
- a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról szóló1/2025. (I. 31.) **SZTFH rendelet,**
- a kiberbiztonsági felügyeleti díjról szóló 2/2025. (I. 31.) **SZTFH rendelet**
- a kiberbiztonsági felügyelet és feladatellátás és a hatósági ellenőrzés lefolytatásának részletes szabályairól, valamint az információbiztonsági felügyelőről szóló 3/2025. (IV. 17.) **SZTFH rendelet**
- a kiberbiztonsági audit végrehajtására jogosult auditorok nyilvántartásáról és az auditorral szemben támasztott követelményekről szóló 7/2024. (VI. 24.) **SZTFH rendelet**

Kérdése van?

Forduljon hozzánk bizalommal!

www.blackcell.io
compliance@blackcell.io