Útmutató a NIS 2 kiberbiztonsági irányelv Intézményi bevezetéséhez

FELSŐVEZETŐI TÁJÉKOZTATÓ ANYAG

Nagy István
Informatikai biztonsági rendszer auditor
Certified GDPR manager
NIS2 referens

Jogszabályi háttér

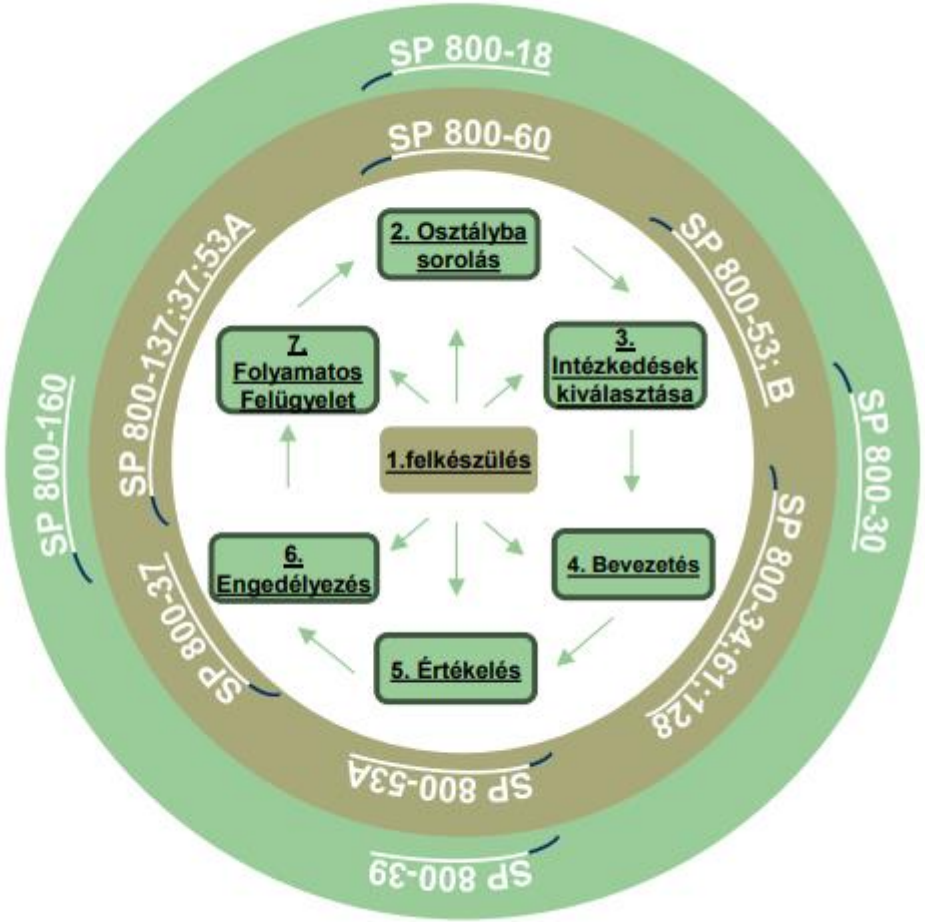
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- Az Európai Parlament és a tanács (EU) 2019/881 rendelete (2019. április 17.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 2019/881 Eu. rendelet az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály);
- 2022 évi 2555 Eu irányelv - az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv);
- 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről;
- 23/2023. SZTFH rendelet az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról
- 10/2023. (V. 15.) SZTFH rendelet az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról;
- 15/2023. (VII. 31.) SZTFH rendelet a Szabályozott Tevékenységek Felügyeleti Hatósága kiberbiztonsági feladataival összefüggő eljárásainak igazgatási szolgáltatási díjairól;
- 305/2023. (VII. 11.) Korm. rendelet a kiberbiztonsági bírságok mértékéről, a bírság kiszabásának és befizetésének részletes eljárási szabályairól.

A **National Institute of Standards and Technology**
(magyarul: *Nemzeti Szabványügyi és Technológiai Intézet (***NIST**)
az Amerikai Egyesült Államok Kereskedelmi Minisztériumának állami felügyelete alá tartozó költségvetési intézménye.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST ökoszisztéma

	NIST
Biztonsági és adatvédelmi intézkedések információs rendszerek és szervezetek részére	800-53
Biztonsági és adatvédelmi intézkedések értékelése	800-53A
Biztonsági osztályok és testreszabási segédlet	800-53B
Rendszerbiztonsági terv segédlet	800-18
Kockázatértékelési segédlet	800-30
Üzletmenet-folytonosság tervezési segédlet	800-34
Risk Management Framework for Information Systems (RMF)	**800-37**
Információbiztonsági kockázatok kezelése	800-39
Incidenskezelési segédlet	800-61
Információ és információs rendszerek biztonsági osztályba sorolása	800-60
Rendszerfejlesztési életciklus	800-64
Information Security Continuous Monitoring (ISCM)	**800-137**
Kiberbiztonsági szempontból ellenálló rendszerek fejlesztése	800-160



A szervezeteknek kellő gondossággal kell kezelniük az információbiztonsági és adatvédelmi kockázatokat egy átfogó kockázatkezelési program létrehozásával.

1. Rendszerek biztonsági osztályba sorolása: Az információs rendszerek osztályozása az alapján, hogy milyen hatással lenne a szervezetre, ha azok sérülnének.
2. Védelmi intézkedések kiválasztása és végrehajtása: Azoknak a biztonsági és adatvédelmi ellenőrzéseknek a kiválasztása és alkalmazása, amelyek megfelelnek a szervezet küldetésének és üzleti igényeinek.
3. A védelmi intézkedések hatékonyságának értékelése: A védelmi intézkedések teljesítményének értékelése annak biztosítására, hogy azok a kívánt védelmet nyújtsák.
4. Rendszerek engedélyezése: A rendszerek hivatalos jóváhagyása az üzemeltetésre, biztosítva, hogy megfeleljenek a biztonsági és adatvédelmi követelményeknek.
5. Folyamatos felügyelet: Állandó felügyelet fenntartása az újonnan felmerülő fenyegetések és sebezhetőségek észlelése és kezelése érdekében.

Ezeknek a lépéseknek a gondos végrehajtásával a szervezetek összehangolhatják tevékenységeiket a vonatkozó törvényekkel, szabályozásokkal, végrehajtási rendeletekkel és kormányzati politikákkal.

A kockázatkezelési keretrendszerek és folyamatok segítenek kialakítani, bevezetni és fenntartani azokat a védelmi intézkedéseket, amelyek megfelelnek az érdekelt felek igényeinek és a jelenlegi fenyegetettségi környezetnek.

Ezek a folyamatok, eljárások, módszerek és technológiák elengedhetetlenek:

- az információs rendszerek megbízhatóságának és ellenálló képességének biztosításához.
- az alapvető küldetési és üzleti funkciók támogatásához.
- a hatékony kockázatalapú stratégiák alkalmazásához mely biztosítja, hogy a szervezet alkalmazkodni tudjon a változó fenyegetésekhez, miközben fenntartja a szigorú biztonsági és adatvédelmi szabványokat.

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/881 RENDELETE (2019. április 17.)

Kiberbiztonság:

Azok a tevékenységek, amelyek a kiberfenyegetésekkel érintett hálózati és információs rendszereknek, az ilyen rendszerek felhasználóinak és más személyeknek a védelméhez szükségesek.

Kiberfenyegetés:

Bármely olyan potenciális körülmény, esemény vagy cselekmény, amely károsíthatja vagy megzavarhatja a hálózati és információs rendszereket, az ilyen rendszerek felhasználóit és más személyeket, vagy azokra egyéb kedvezőtlen hatást gyakorolhat.

IKT fogalma:

Az „Információs és Kommunikációs Technológiák” olyan eszközök, technológiák, szervezési tevékenységek, innovatív folyamatok összessége, amelyek az információ- és a kommunikációközlést, feldolgozást, áramlást, tárolást, kódolást elősegítik, gyorsabbá, könnyebbé, és hatékonyabbá teszik.

IKT-termék:

Valamely hálózati vagy információs rendszer eleme vagy elemeinek csoportja.

IKT-szolgáltatás:

Olyan szolgáltatás, amely teljes mértékben vagy legnagyobb részben információ hálózati és információs rendszerek útján történő továbbításából, tárolásából, lekérdezéséből vagy kezeléséből áll.

IKT-folyamat:

Valamely IKT-termék vagy IKT-szolgáltatás tervezése, fejlesztése, rendelkezésre bocsátása illetve nyújtása vagy karbantartása céljából végzett tevékenységek összessége.

Mi számít egy elektronikus információs rendszernek?

Egy elektronikus információs rendszernek kell tekinteni az azonos célból kezelt adatok kezelésében, feldolgozásában résztvevő erőforrások (technikai eszközök, személyek, eljárási szabályok) együttesét.

Ennek alapján:

- Több elektronikus információs rendszernek lehetnek közös rendszerelemei.
- Egy elektronikus információs rendszernek lehetnek külső közreműködő tulajdonában álló rendszerelemei.

Kinek kell elvégeznie a biztonsági osztályba sorolást, ha az elektronikus információs rendszert az érintett szervezet központosított hírközlési vagy informatikai szolgáltatón szolgáltatásán keresztül veszi igénybe?

- Az igénybe vevő adatgazda szervezetnek és az adatkezelő minőségben közreműködő szolgáltatónak (együtt érintettek) külön-külön a saját információbiztonsági kockázata alapján el kell végeznie a biztonsági osztályba sorolást. [187/2015. (VII. 13.) Korm. rendelet 11. § (4) bekezdés]
- Az érintetteknek kétoldalú szolgáltatási megállapodásban kell rögzíteniük, hogy egymás kockázatának kezelésében milyen feladatmegosztás szerint vesznek részt. [Ibtv. 11. § (3) bekezdés]

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

19. § (1) Az érintett szervezet a kiberfenyegetések által okozható károk mértékével arányos módon köteles gondoskodni az elektronikus információs rendszerei és azok fizikai környezetének a biztonságáról.

(2) Az (1) bekezdés szerinti biztonság magában foglalja az elektronikus információs rendszerek, valamint fizikai környezetük védelmét minden olyan eseménytől, amely veszélyeztetheti

a) a tárolt, továbbított vagy feldolgozott adatok, információk, vagy

b) az elektronikus információs rendszerek által nyújtott vagy azon keresztül elérhető szolgáltatások bizalmasságát, sértetlenségét és rendelkezésre állását.

(3) A (2) bekezdésben meghatározott védelemnek ki kell terjednie:

a) az információbiztonsági irányítás rendszerére,

b) az elektronikus információs rendszerek kockázatainak feltárására és kezelésére,

c) a kockázatok csökkentésére irányuló, a szervezet kockázatelemzésében rendszerenként meghatározandó biztonsági osztálynak megfelelő adminisztratív, logikai és fizikai intézkedések alkalmazására,

d) a biztonsági események megelőzésére, felismerésére, kezelésére és hatásainak csökkentésére,

e) az üzletmenet folytonosság biztosítására és

f) az elektronikus információs rendszerek és az ezek által használt szoftver és hardver termékek beszerzésére, fejlesztésére, és üzemeltetésére.

(4) Ha az érintett szervezet az elektronikus információs rendszer létrehozásában, üzemeltetésében, karbantartásában vagy javításában közreműködőt vesz igénybe, a (3) bekezdés szerinti követelményeknek a közreműködő esetében is teljesülniük kell.

(5) Az érintett szervezet vezetője köteles gondoskodni arról, hogy az (1)–(3) bekezdés szerinti követelményeket a (4) bekezdés szerinti közreműködő tekintetében szerződésbe foglalják.

(6) Az érintett szervezet vezetője

a) meghatározza az elektronikus információs rendszerek biztonságáért felelős személy feladatait és felelősségi körét,

b) meghatározza az elektronikus információs rendszerek felhasználóira vonatkozó szabályokat, és

c) gondoskodik a szervezet munkatársai rendszeres információbiztonsági képzéséről és ismereteinek szintentartásáról.

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

20. § (1) Az érintett szervezet köteles az elektronikus információs rendszereket, valamint az azon tárolt, továbbított vagy feldolgozott adatokat a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter rendeletében meghatározott szempontrendszer alapján biztonsági osztályba sorolni.
(2) A biztonsági osztályba sorolás eredményeként a bizalmasság, a sértetlenség, a rendelkezésre állás sérülésének kockázata alapján „alap”, „jelentős” vagy „magas” biztonsági osztályt kell alkalmazni.
(3) Az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedéseket a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter rendeletben határozza meg.
(4) A 19. § (1)–(4) bekezdésében meghatározott egyes követelményeknek való megfelelés igazolására – ha rendelkezésre áll – európai vagy nemzeti kiberbiztonsági tanúsítási rendszer alapján tanúsított IKT-termék, IKT-szolgáltatás vagy IKT-folyamat alkalmazható.
(5) Az SZTFH elnökének rendeletében meghatározott érintett szervezetek kötelesek az európai vagy nemzeti kiberbiztonsági tanúsítási rendszer alapján tanúsított, az SZTFH elnökének rendeletében meghatározott IKT-terméket, IKT-szolgáltatást vagy IKT-folyamatot használni.

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

1. §

…

(2) A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (a továbbiakban: Kibertantv.) hatálya alá tartozó elektronikus információs rendszert a Kibertantv. szerinti érintett szervezet (a továbbiakban: érintett szervezet) az 1. mellékletben felsorolt szempontok szerint sorolja biztonsági osztályba.

..

3. § (1) Az 1. § (2) bekezdésében foglaltak szerint elvégzett besorolás alapján az érintett szervezet a 2. mellékletben meghatározott, az elektronikus információs rendszerére érvényes biztonsági osztályhoz rendelt követelményeket az abban meghatározott módon teljesíti.

(2) Az érintett szervezetre és elektronikus információs rendszereire az e rendelet előírásai szerint kidolgozott szabályzatokban meghatározott adminisztratív, logikai és fizikai védelmi intézkedések irányadóak. Ha ezen intézkedésektől egy elektronikus információs rendszer esetében a szervezet által elvégzett kockázatelemzés alapján indokolt eltérni, akkor az 1. mellékletben meghatározottak szerint kell eljárni.

(3) Ha az érintett szervezet rendelkezési joga az elektronikus információs rendszernek csak egyes elemeire vagy funkcióira terjed ki, a 2. mellékletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni.

(4) Az érintett szervezet a kockázatelemzés és a kockázatok kezelése körében azonosítja és dokumentálja az elektronikus információs rendszer bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket a 3. mellékletben foglalt fenyegetéskatalógus elemeinek vizsgálatával.

A KOCKÁZATMENEDZSMENT KERETRENDSZER 1.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény hatálya alá tartozó elektronikus információs rendszerrel rendelkező szervezet a biztonsági osztályba sorolás és a védelmi intézkedések bevezetésének támogatására kockázatmenedzsment keretrendszert működtet, amelynek keretében a szervezetre vonatkozóan meghatározza és dokumentumban rögzíti:

1. Kockázatmenedzsment keretrendszer
   - az elektronikus információszerepköröket, felelősségeiket, feladataikat és az ehhez szükséges hatásköröket,ós rendszerei védelmével kapcsolatos
   - a kockázatmenedzsment stratégiáját, amely leírja, hogy a szervezet hogyan azonosítja, értékeli, kezeli és felügyeli a biztonsági kockázatokat,
   - a védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó biztonságfelügyeleti stratégiát, amely magába foglalja a védelmi intézkedésekhez kapcsolódó tevékenységek ellenőrzésének gyakoriságát, felügyeletének módszereit és eszközeit,
   - az elektronikus információs rendszerekre (EIR) vonatkozóan nyilvántartást vezet.
2. Meghatározott irányelvek szerint biztonsági osztályba sorolja az elektronikus információs rendszereit
3. Beazonosítja a biztonsági osztályhoz tartozó védelmi intézkedéseket. A beazonosított intézkedéseket a kockázatkezelés alapján testre szabja ezáltal megállapítja az EIR-re értelmezendő és alkalmazandó biztonsági követelményeket.
4. A 3 pontban meghatározott biztonsági követelményeket „Rendszerbiztonsági terv”-ben dokumentálja. A tervet a szervezet vezetője és/vagy az IBF hagy jóvá.
5. A folyamatos felügyeleti stratégia érdekében kidolgozásra kerül a folyamatos ellenőrzésre vonatkozó eljárásrend.
6. Rangsorolásra és végrehajtásra kerülnek a ”Rendszerbiztonségi terv”-ben jóváhagyott intézkedések.

A KOCKÁZATMENEDZSMENT KERETRENDSZER 2.

7. Értékelésre kerülnek a Rendszerbiztonsági tervben előírt és elvégzett intézkedések.
   - Meghatározásra kerülnek a védelmi intézkedések értékeléséért felelős személyek.
   - A védelmi intézkedések értékelési terve kialakításra kerül.
   - Értékelésre kerülnek a védelmi intézkedések.
   - Az észrevételek alapján elkészül az értékelési jelentés.
   - Intézkedési terv a fennmaradó intézkedésekre.
   - A rendszer biztonsági állapotára vonatkozó dokumentumok (rendszerbiztonsági terv, értékelési jelentés, rendszer kockázatelemzés, intézkedési terv) alapján az üzembe helyezésére vagy üzemben tartására vonatkozó kockázatokat megvizsgálja, és a szervezet vezetője más személyre át nem ruházható feladatkörében eljárva – jegyzőkönyvben dokumentált módon – dönt a rendszer használatbavételéről vagy használatának folytatásáról
8. Az EIR teljes életciklusa alatt gondoskodik arról, hogy a rendszerben vagy a működési környezetben bekövetkező a rendszer biztonsági helyzetét befolyásoló változások esetén:
   - A dokumentáció frissítésre kerüljön.
   - A védelmi intézkedések állapota rendszeresen ellenőrzésre és jelentésre kerüljön.
   - A biztonság állapotának felülvizsgálata (kockázatok ellenőrzése).
   - Az éles üzemből való kivonás tervezése. A kivonás kapcsán felmerülő kockázatok kezelése.

BIZTONSÁGI OSZTÁLYBA SOROLÁS

A jogszabályban meghatározott biztonsági osztályba sorolás elvégzése a szervezet felelőssége.

1. **Az „alap” biztonsági osztály esetében legfeljebb csekély káresemény következhet be**.
   - az elektronikus információs rendszerben jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet,
   - a szervezet üzleti vagy ügymenete szempontjából csekély értékű vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet,
   - a lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető,
   - a közvetlen és közvetett anyagi kár a szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg.

2. **A „jelentős” biztonsági osztály esetében közepes káresemény következhet be**.
   - nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet,
   - személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket),
   - a szervezet üzleti vagy ügymenete szempontjából érzékeny folyamatokat kezelő rendszer, információt képező adat vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet,
   - a káresemény lehetséges társadalmi-politikai hatásai a szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni,
   - a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át.

3. **A „magas” biztonsági osztály esetében nagy káresemény következhet be.**
   - különleges személyes adat nagy mennyiségben sérülhet,
   - emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,
   - nemzeti adatvagyon helyreállíthatatlanul megsérülhet,
   - az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított,
   - a szervezet üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet,
   - súlyos bizalomvesztés állhat elő a szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek,
   - a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 10%-át.

Elektronikus információs rendszerekre vonatkozó nyilvántartás minimálisan elvárt tartalma

- A rendszer megnevezése,
- A rendszer által támogatandó üzleti célok, funkciók és folyamatok (1.1.1.2.1),
- A tervezésben, fejlesztésben, implementálásban, üzemeltetésben, karbantartásban, használatban és ellenőrzésben érintett személyek vagy szervezetek (1.1.1.2.2),
- Az érintett vagyonelem/rendszerelem (1.1.1.2.3),
- A rendszer szervezeti és technológiai határa (1.1.1.2.4),
- A rendszer által feldolgozandó, tárolandó és továbbítandó adatköröket és azok életciklusát (1.1.1.2.5),
- A rendszerrel kapcsolatos fenyegetettségből adódó biztonsági kockázatok értékelését és kezelését az elvárt elvek szerint (1.1.1.2.6),
- A rendszer helyét a szervezeti architektúrában, amennyiben a szervezet rendelkezik vele (1.1.1.2.7);

KOCKÁZATELEMZÉS ÉS A KOCKÁZATOK KEZELÉSE

1. A szervezet értékeli az elektronikus információs rendszerrel, az általa kezelt adatokkal kapcsolatosan felmerülő kockázatokat:
   - Azonosítja és dokumentálja az elektronikus információs rendszer és az általa feldolgozott adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket. Az azonosítás során legalább a fenyegetés katalógus elemeit vizsgálja.
   - Azonosítja a sérülékenységeket és a hajlamosító körülményeket, amelyek befolyásolják annak valószínűségét, hogy a fenyegetések a szervezeti vagyonelemek, személyek, vagy más szervezetek számára káros hatásokhoz vezetnek.
   - Meghatározza annak a valószínűségét, hogy az azonosított fenyegetések a szervezeti vagyonelemek, folyamatok, személyek vagy más szervezetek számára káros hatásokat eredményeznek-e, figyelembe véve az azonosított sérülékenységeket és körülményeket, valamint a szervezet a fenyegetések kihasználhatóságával kapcsolatosan végrehajtott ellenintézkedéseit.
   - Meghatározza a fenyegetések szervezeti vagyonelemekre, személyekre, vagy más szervezetekre vonatkozó lehetséges káros hatásait és azok mértékét.
   - Meghatározza a fenyegetések káros hatásainak és azok bekövetkezésének valószínűsége alapján az eredő kockázatokat, valamint legalább négy fokozatú skálán („alacsony”, „közepes”, „magas”, „kritikus”) azok mértékét (kockázati kategória).
   - Dokumentálja és a szervezeti döntéshozók számára kommunikálja a kockázatelemzés eredményét a kockázatkezelési válaszlépések támogatása érdekében, valamint biztosítja a kockázatelemzési folyamat során keletkezett információk megosztását az arra jogosultakkal.
2. A szervezet az azonosított kockázatok esetében eldönti és dokumentumban rögzíti, hogy az egyes kockázatok kezelése érdekében az alábbiak közül egyenként mely intézkedést alkalmazza:
   - kockázat elkerülése (például az elektronikus információs rendszer vagy a rendszerelemének, funkciójának használatból való teljes körű kivezetésével),
   - kockázat csökkentése védelmi intézkedések kialakításával és működtetésével,
   - kockázat áthárítása vagy megosztása harmadik felekkel,
   - kockázat felvállalása.
3. Biztosítja, hogy kizárólag a legalacsonyabb kockázati kategóriába eső kockázatok esetén alkalmaz részletes indoklás nélkül kockázatfelvállalást. Az ennél magasabb kategóriába eső kockázatok esetén az egyes kockázatok felvállalását a szervezet vezetője vagy a kockázatok kezeléséért felelős szerepkört betöltő személy kockázatonként történő indoklás mellett hagyja jóvá.
   - A kockázatelemzés eredményét felhasználja az elektronikus információs rendszer biztonsági osztálya megállapításának, valamint a védelmi intézkedések kiválasztásának és testre szabásának támogatására.
   - Végrehajtja, értékeli és felügyeli a kockázatcsökkentő védelmi intézkedéseket.
4. A szervezet folyamatosan nyomon követi az elektronikus információs rendszerrel kapcsolatos kockázatok változásaihoz hozzájáruló tényezőket, és ennek alapján frissíti és naprakészen tartja a kockázatelemzési dokumentumait.

Büntetési tételek

A Kibertan. tv. és egyéb magyar NIS2 jogszabályok megsértésére vonatkozó a felügyeleti hatóság által kiszabható szankciók mértékét a 305/2023. a kiberbiztonsági bírságok mértékéről, a bírság kiszabásának és befizetésének részletes eljárási szabályairól szóló rendelet 1. melléklete határozza meg.

Az érintett szervezet a kiszabott NIS2 bírságot 8 napon belül köteles megfizetni, több szabálysértés együttes érvényesülése esetén a legnagyobb kiszabható szankció az egyes szabálytalanságok kiszabható legmagasabb bírságának összege. A bírság a határidő leteltét követően újra kiszabható.

A NIS2 követelmények nem teljesítése esetén a kibertan.tv-ben szereplő szabályozás szerint a tanúsító hatóság határidő kitűzésével felszólítja a szervezetet a hiányosság javítására. Amennyiben ennek ellenére sem teljesíti a követelményekben megszabottakat, így a hatóság a szabálytalanság mértékével arányos büntetést szabhat ki, amely további nemteljesítés esetén megismételhető.

„2. § (1) A kiszabott bírságot a tanúsító hatóság határozatának véglegessé válását követő 8 napon belül kell megfizetni a tanúsító hatóság határozatban megjelölt, Magyar Államkincstárnál vezetett számlájára.

(2) Több szabálytalanság együttes fennállása esetén a bírság kiszabható legnagyobb mértéke az egyes szabálytalanságokért kiszabható bírságok legnagyobb mértékének összege.

(3) A bírság ugyanazon tényállás mellett a Kibertan.tv. 15. § (1) bekezdése alapján meghatározott határidő eredménytelen elteltét követően ismételten kiszabható.”

305/2023. (VII. 11.) Korm. rendelet a kiberbiztonsági bírságok mértékéről, a bírság kiszabásának és befizetésének részletes eljárási szabályairól

Az egyes szabálytalanságok miatt kiszabható bírság mértéke

	A	B	C
1.	A szabálytalanság megnevezése	A bírság legkisebb mértéke forintban meghatározva	A bírság legnagyobb mértéke forintban meghatározva
2.	Megfelelőségi önértékelés esetén az uniós megfelelőségi nyilatkozatnak az (EU) 2019/881 európai parlamenti és tanácsi rendelet 53. cikk (3) bekezdésében előírt megküldési kötelezettség nemteljesítése a tanúsító hatóság és az Európai Uniós Kiberbiztonsági Ügynökség részére	50 000	100 000
3.	Megfelelőségi önértékelés esetén a Kibertan.tv. 11. § (3) bekezdésében előírt dokumentumok megküldésére vonatkozó kötelezettség nemteljesítése a tanúsító hatóság részére	50 000	100 000
4.	A Kibertan.tv. 12. §-ában foglalt feltételeknek nem megfelelő szervezet általi megfelelőségértékelési tevékenység végzése	1 000 000	50 000 000
5.	Megfelelőségi jelölés Kibertan.tv. 10. § (2) bekezdése szerinti jogosulatlan használata	300 000	50 000 000
6.	A Kibertan.tv. 14. § (5) bekezdése szerinti adatszolgáltatás elmulasztása	50 000	5 000 000
7.	A Kibertan.tv. 9. § (3) bekezdésében meghatározott, a sebezhetőség vagy rendellenesség bejelentésére irányuló kötelezettség teljesítésének elmulasztása	300 000	5 000 000
8.	Az A:2–A:7 mezőben nem szereplő, a tanúsító hatóság által feltárt, a Kibertan.tv. 15. § (1) bekezdése szerinti hiányosságok alapján a szükséges módosítások végrehajtásának, intézkedések megtételének elmulasztása	200 000	10 000 000