Mi történik, ha nem felel meg egy cég az auditon?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/27

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.27	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Amennyiben egy szervezet a NIS2 követelmények szerinti kiberbiztonsági auditon nem felel meg, az auditor ezt jelentésben rögzíti és értesíti a felügyeleti hatóságot (SZTFH). A „nem megfelelt" minősítés akkor kerül megállapításra, ha a szervezet biztonsági intézkedései és folyamatai nem biztosítják az előírt védelmi szintet.

Hatósági következmények:

- felügyeleti eljárás indítása,
- kötelezés a hiányosságok megszüntetésére és intézkedési terv benyújtására,
- ismételt ellenőrzések és fokozott felügyelet.

Megfeleléshez szükséges lépések:

- nem megfelelőségek feltárása és ütemezett korrekciós terv végrehajtása,
- kockázatelemzés és biztonsági besorolás felülvizsgálata,
- hiányzó technikai és szervezeti kontrollok bevezetése,
- sérülékenységek megszüntetése és védelmi intézkedések megerősítése.

Lehetséges szankciók tartós vagy súlyos mulasztás esetén:

- jelentős bírságok, akár a szervezet vezetőjével szemben is,
- működési engedély ideiglenes korlátozása vagy felfüggesztése,
- vezető tisztségviselő ideiglenes eltiltása,
- a jogsértés nyilvánosságra hozatala és reputációs károk.

A sikertelen audit nem végállapot, hanem kötelező korrekciós folyamat kezdete. A megfelelés elmaradása azonban jogi, pénzügyi és működési kockázatokat hordoz, valamint közvetlen vezetői felelősséget is felvet.

2. A VIZSGÁLANDÓ KÉRDÉS

- Mi történik, ha nem felel meg egy cég az auditon?
- Milyen lépéseket kell végrehajtania a megfeleléshez?
- Milyen szankciókra számíthat?

3. VÁLASZ

3.1 A sikertelen audit következményei

Amennyiben egy szervezet a kiberbiztonsági audit során nem felel meg a jogszabályi követelmények jelentős részének, és az audit eredménye sikertelen, az auditor ezt rögzíti az auditjelentésben, valamint az eredményről értesíti a felügyeleti hatóságot (Szabályozott Tevékenységek Felügyeleti Hatósága – SZTFH).

Az 1/2025. (I. 31.) SZTFH rendelet – a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról (a továbbiakban: Audit rendelet) – az auditort jelentési kötelezettséggel terheli a Hatóság felé. Az Audit rendelet 5. mellékletének 2.2. és 2.3. pontja alapján, ha az elektronikus információs rendszerek (EIR) értékelése során a Szervezet Ellenálló-Képességi Indexe (SZEKI) vagy a Védelmi Megfelelési Index (VMI) 70% alatt van, az „nem felel meg" vagy „nem megfelelt" minősítést von maga után.

> „(8) *Az auditor a (7) bekezdés szerinti auditjelentést, valamint annak a Hatóság által a honlapján meghatározott, gépi feldolgozást biztosító specifikáció szerinti változatát haladéktalanul, de legkésőbb az auditjelentés kiállítását követő 7 napon belül megküldi a Hatóság részére." [1/2025. (I. 31.) SZTFH rendelet 5. § (8) bekezdés]*

A 2024. évi LXIX. törvény – Magyarország kiberbiztonságáról (a továbbiakban: Kiberbiztonsági tv.) – értelmében sikertelen auditot követően a hatóság felügyeleti eljárást indíthat, és kötelezheti a szervezetet a hiányosságok pótlására.

> *„(1) Ha a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a biztonsági hiányosságokat nem hárítja el, a megfeleléshez szükséges intézkedések meghozatalát elmulasztja, vagy a tevékenységet nem hagyja abba, a kiberbiztonsági hatóság [...] felszólítja a követelmények, az ellenőrzés vagy az audit során feltárt vagy tudomására jutott biztonsági hiányosságok elhárítására vagy a megfeleléshez szükséges intézkedések meghozatalára [...]" [2024. évi LXIX. törvény 30. § (1) bekezdés a) pont]*

3.2 A megfeleléshez szükséges lépések végrehajtása

A szervezetnek a hiányosságok feltárását követően strukturált folyamaton kell végigmennie a megfelelés elérése érdekében. Ez magában foglalja a kockázatelemzés felülvizsgálatát, intézkedési terv készítését és a konkrét védelmi intézkedések bevezetését.

3.2.1 Hiányosságok elemzése és Intézkedési terv készítése

A szervezetnek az auditjelentés alapján azonosítania kell a nem megfelelőségeket, és ezek javítására ütemezett intézkedési tervet kell kidolgoznia.

> *„5.10. A szervezet: [...] 5.10.1. Intézkedési tervet dolgoz ki, amelyben mérföldköveket határoz meg az EIR-ben tervezett korrekciós intézkedések dokumentálására, hogy a védelmi intézkedések értékelése során feltárt gyengeségeket vagy hiányosságokat kijavítsák, valamint a rendszer ismert sérülékenységeit csökkentsék vagy megszüntessék." [7/2024. (VI. 24.) MK rendelet 2. melléklet 5.10. pont] (Alap: X, Jelentős: X, Magas: X)*
> *„1.1.5.5. az értékelési jelentésben foglalt észrevételek és javaslatok alapján a szervezet további intézkedéseket vezet be a követelmények teljesítése*

érdekében, majd újraértékeli a védelmi intézkedéseket, valamint intézkedési tervet készít a fennmaradó kockázatok kezelésére;" [7/2024. (VI. 24.) MK rendelet 1. melléklet 1.1.5.5. pont]

3.2.2 Kockázatelemzés és biztonsági osztályba sorolás felülvizsgálata

Előfordulhat, hogy a nem megfelelés oka a téves biztonsági osztályba sorolás vagy a hiányos kockázatelemzés.

„(4) A 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. melléklet szerinti fenyegetéskatalógus elemeinek vizsgálatával." [7/2024. (VI. 24.) MK rendelet 2. § (4) bekezdés]

3.2.3 Konkrét védelmi intézkedések pótlása

A hiányzó kontrollokat a 7/2024. (VI. 24.) MK rendelet 2. melléklete, azaz a Védelmi intézkedések katalógusa alapján kell pótolni. Kiemelt figyelmet kell fordítani azokra a területekre, amelyek gyakran okoznak nem megfelelőséget.

3.3 Várható szankciók

Amennyiben a szervezet nem tesz eleget jogszabályi kötelezettségeinek, vagy az SZTFH felszólítása ellenére nem hárítja el a hiányosságokat, a Kiberbiztonsági törvény jogkövetkezményeket helyez kilátásba.

A hatóság tájékoztatása szerint szankciókat csak kirívó esetekben, a szándékos vagy súlyosan gondatlan jogsértés esetén alkalmaznak. A nem megfelelés önmagában nem von magával szankciót, ha a szervezet a Hatóság által megállapított határidőben pótolja a hiányosságokat.

3.3.1 Bírság

A hatóság mérlegelés alapján bírságot szabhat ki, amelynek összege a jogsértés súlyától függően változhat.

> *„Ha az (1) bekezdés szerinti intézkedések alkalmazása ellenére az érintett szervezet a jogszabályokban foglalt biztonsági követelményeket vagy az ehhez kapcsolódó eljárási szabályokat nem teljesíti vagy nem tartja be, a biztonsági hiányosságokat nem hárítja el, a megfeleléshez szükséges intézkedések meghozatalát elmulasztja, vagy a tevékenységet nem hagyja abba, a kiberbiztonsági hatóság az eset összes körülményének mérlegelésével kormányrendeletben meghatározott mértékű bírságot szabhat ki.” [2024. évi LXIX. törvény 30. § (2) bekezdés]*

A szervezet vezetője is bírságolható:

> *„Ha a szervezet vezetője a jogszabályban előírt kötelezettségének nem tesz eleget, a nemzeti kiberbiztonsági hatóság az eset összes körülményének mérlegelésével kormányrendeletben meghatározott mértékű bírsággal sújthatja, ismételt jogsértés esetén sújtani köteles.” [2024. évi LXIX. törvény 30. § (3) bekezdés]*

3.3.2 Tevékenységtől való eltiltás és engedély felfüggesztése (Alapvető szervezetek esetén)

Különösen súlyos szankció, hogy a hatóság kezdeményezheti az alapvető szolgáltatást nyújtó szervezet tevékenységi engedélyének felfüggesztését.

> *„(6) Ha a nem közigazgatási szervnek minősülő alapvető szervezet a kiberbiztonsági hatóság által szabott határidőn belül nem tesz eleget a hatósági kötelezésnek, a kiberbiztonsági hatóság [...] kezdeményezheti az illetékes hatóságnál az alapvető szervezet által nyújtott, a jogsértéssel érintett alapvető szolgáltatások vagy tevékenységek egészére vagy egy részére vonatkozó tanúsítás vagy engedély ideiglenes felfüggesztését [...]” [2024. évi LXIX. törvény 30. § (6) bekezdés a) pont]*

3.3.3 Vezető tisztségviselő eltiltása (Alapvető szervezetek esetén)

Az alapvető szervezetek esetében a hatóság kezdeményezheti a vezető tisztségviselő eltiltását a vezetői feladatok ellátásától.

„[...] a kiberbiztonsági hatóság [...] kezdeményezheti a cégbíróságnál az alapvető szervezet vezetőjének az adott szervezetben betöltött vezető tisztségviselői feladatainak ellátásától való ideiglenes eltiltását.” [2024. évi LXIX. törvény 30. § (6) bekezdés b) pont]

3.3.4 Nyilvánosságra hozatal

A hatóság kötelezheti a szervezetet arra, hogy a jogsértés tényét hozza nyilvánosságra, amely jelentős reputációs kárt okozhat.

„(5) A kiberbiztonsági hatóság [...] kötelezheti a szervezetet arra, hogy a jogszabálysértés tényét és körülményeit a kiberbiztonsági hatóság által meghatározott módon, az adatvédelmi és az üzleti titokra vonatkozó szabályokat figyelembe véve hozza nyilvánosságra [...]” [2024. évi LXIX. törvény 30. § (5) bekezdés a) pont]

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról