Sikertelen audit után hogyan készítsünk intézkedési tervet?

VFP2 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/13

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.08.14	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

A Szabályozott Tevékenységek Felügyeleti Hatósága által véleményezett dokumentum

1 VEZETŐI ÖSSZEFOGLALÓ

A sikertelen kiberbiztonsági auditot követően a szervezet köteles intézkedési tervet készíteni a feltárt hiányosságok megszüntetésére. Az intézkedési terv célja, hogy átlátható módon bemutassa a tervezett javító intézkedéseket, azok felelőseit, végrehajtási határidejét, valamint a teljesítés igazolásának módját. Az intézkedési terv alapján a szervezet folyamatosan képes nyomon követni a hiányosságok megszüntetésének előrehaladását, amiről szükség esetén a Hatóságot is értesíteni tudja. A Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH) azon szervezetek esetében, melyeknek a szervezet ellenálló-képességi index (a továbbiakban: SZEKI) „nem megfelelt" értékelést kapott cselekvési terv készítésére szólítja fel a szervezetet. A cselekvési tervben szereplő feladatok előre haladásáról a szervezetnek negyedévente tájékoztatnia kell a Hatóságot. Az SZTFH az intézkedési terv alapján folyamatosan nyomon követi a hiányosságok megszüntetésének előrehaladását. Az intézkedési tervnek reális, végrehajtható és nyomon követhető intézkedéseket kell tartalmaznia, valamint azt az arra jogosult felsővezetőnek jóvá kell hagynia. A dokumentum nem projektterv vagy részletes műszaki leírás, hanem vezetői szintű nyilvántartás, amely alkalmas a végrehajtás státuszának követésére és a megfelelőség igazolására.

Azt, hogy mit a teendő akkor, ha a szervezet nem felelt meg az auditon egy korábbi MKIK állásfoglalás tartalmazza: **https://nis2.mkik.hu/jogi-allasfoglalasok/27**

2 A VIZSGÁLANDÓ KÉRDÉS

A sikertelen auditot követően a Szervezetnek intézkedési tervet kell készíteni, amelyben meghatározza miként fogja az audit során megállapított hiányosságokat kezelni.

Milyen paramétereknek kell megfelelni egy Intézkedési tervnek?

Milyen információt kell tartalmaznia?

3 VÁLASZ

3.1 Az Intézkedési terv szerepe

Az Intézkedési terv szerves része az információbiztonsági irányítási rendszernek, már az audit előtt is. Alapjául a Szervezet által elvégzett biztonsági értékelések, kockázatelemzések, sérülékenységvizsgálatok, valamint a folyamatos felügyeleti tevékenységek során feltárt hiányosságok szolgálnak. A szabályozás megköveteli a meglétét a Programmenedzsment, valamint az Értékelés, engedélyezés, monitorozás követelménycsaládok esetében. A kiberbiztonsági audit során is vizsgálják a meglétét és a tartalmát olyan szempontból, hogy a szervezet tervezett korrekciós intézkedései milyen módon biztosították a védelmi intézkedések értékelése során feltárt gyengeségek vagy hiányosságok kijavítását, valamint a rendszer ismert sérülékenységeinek kezelését vagy azok megszüntetését.

3.2 Sikertelen audit utáni Intézkedési terv

Az auditot követően a vizsgált szervezetnek új Intézkedési tervet kell készítenie, valamint, amennyiben a SZEKI értéke „nem megfelelt”, vagyis 70 alatti értéket ért el, az SZTFH cselekvési terv készítésére szólítja fel. Az két dokumentum, csupán elnevezésében különbözik elsődleges céljuk annak bemutatása, hogy

- a szervezet megértette az audit során feltárt hiányosságokat
- azok kockázatát értékelte
- meghatározta a szükséges javító intézkedéseket
- kijelölte a felelősöket
- **reális ütemezést** készített
- és képes nyomon követni a végrehajtást

Az SZTFH számára küldendő cselekvési terv azonban nem egy egyszeri dokumentum, hanem a megfelelőség helyreállításának nyomon követésére szolgáló eszköz, melyről 90 naponta beszámolási kötelezettség terheli a szervezetet. Az intézkedési tervet is folyamatosan szükséges felülvizsgálni annak érdekében, hogy az abban szereplő feladatok előrehaladása naprakészen nyomon követhető legyen a szervezet, illetve az auditorok számára is.

3.3 Jó Intézkedési terv ismérvei

A hiányosság megfogalmazása	A hiányosságok kontroll vagy elemi kontroll szinten visszakövethetők az audit jelentésből, érdemes az audit jelentés alapján akár elemi kontroll szintig is lebontani a cselekvési tervet a szervezetnél, hiszen amennyiben az auditor a “Cél” megfogalmazását hiányolta az eljárásrendből azt egyértelmű feladatként meg lehet fogalmazni, míg a kontroll, hogy legyen IBSZ egy sokkal nagyobb feladat melynek a szervezet valószínűleg megfelelt. A hatóság nem kéri ilyen részletességgel az Intézkedési tervet, de a szervezet számára nem árt dokumentum, EIR szintű részletes feladatlistát készítenie.
Intézkedés megfogalmazása	Az egy-két szavas válaszok (a szervezete kijavítja, megoldja, elkészíti) helyett röviden, de érthetően legyen ismertetve hogyan fogja a szervezet megszüntetni a felvetett problémát, hivatkozva akár a dokumentum nemére melyben a változtatást meg kell tenni, illetve a rendszerelemre melynek konfigurációját le kell menteni.
Mérföldkövek	Az egyszerűbb önálló feladatoknál (pl. szabályozás elkészítése, oktatás megtartása, nyilvántartás létrehozása) elégséges végcél dátum feljegyzése, azonban az összetettebb feladatoknál (több hónapig tartanak, több szervezeti egységet érintenek, külső beszállítót igényelnek, egymásra épülő

	feladatokból állnak,) célszerű meghatározni ezeket, illetve a feladatok sorrendiségét is. **NE FELEDJÜK! Egyes esetekben – például szabályozás módosulása esetén szükség van a szabályozás újabb elfogadására, kihirdetésére, megismertetésére esetleg oktatására. Ezen feladatokat nem feltétlenül KELL feltüntetni az intézkedési tervben ugyanakkor a következő auditon ezen bizonyítékokat is kérni fogják.**
Határidők	A határidők legyenek reálisak, indokolhatóak, vegyék figyelembe a beszerzéseket, fejlesztéseket, partnereket, a határidő lehetőleg az SZTFH által elvárt következő audit előtt legyen. Ettől természetesen el lehet térni például teljes rendszercsere vagy infrastruktúra szolgáltató esetén, mely projektek akár végződhetnek a következő audit után is, ugyanakkor ez esetekben mindenképpen javasolt mérföldkövek meghatározása.
Függőségek (opcionális)	Mivel egyes feladatok például az incidenskezelési szabályozás oktatása csak a szabályozás készítése után kerülhet végrehajtásra, ezeket a feladatokat javasolt jelölni, vagy legalább valahogyan csoportosítani, de a hatóság számára nem kötelező. Ezek akkor igazán fontosak amikor egy csúszás miatt több határidőt is át kell tervezni.
Felelős	Munkakör megnevezése csak akkor megfelelő amennyiben az adott munkakört betöltő emberből csak egy van, egyébként nem megfelelő, fontos, hogy az intézkedés mindenképp személyhez köthető legyen. A végső felelős minden esetben a szervezet legfelsőbb vezetője, de igyekezzünk olyan felelőst megnevezni, aki a szakmai munkát konkrétan el tudja végezni, vagy közvetlen beosztottjaival el tudja végeztetni. Például egy rendszerbiztonsági terv elkészítéséért lehet felelős egy rendszergazda is.
Bizonyíték (opcionális)	Minden intézkedéshez meg javasolt a szervezet számára legalább házon belül meghatározni, hogyan bizonyítható a végrehajtás annak érdekében, hogy a következő auditra már ez a segítség is előálljon, ugyanakkor egy hatósági intézkedési tervben ezt biztosan nem fogja kérni a hatóság. • jóváhagyott szabályzat • képernyőkép • naplóbejegyzés • teszt jegyzőkönyv • szerződés • stb..

A cselekvési, illetve intézkedési tervnek pedig a szervezet felső vezetőjének, illetve az arra jogosult vezetőjének jóváhagyását kell bírnia.

Az intézkedési terv nem zárul le azzal, hogy elkészítésre, majd elküldésre került, ez egy úgynevezett élő dokumentum. Elvárt a **rendszeres** státuszfrissítés, az esetleges késedelmek indoklása, valamint a határidő módosítások dokumentálása.

3.4 Szakmai ajánlás

Az intézkedési tervet célszerű projektként kezelni, ennek megfelelően ajánlott projektvezetőt kijelölni a koordinációra és eszkalációra, rendszeres vezetői státuszjelentéseket készíteni. A tervnek tükröznie kell a szervezet tényleges végrehajtási képességét; túlzottan optimista vagy nem teljesíthető határidők megadása – és azok rendszeres tologatása - hosszabb távon a hatósági felügyeleti eljárás során kedvezőtlenebb megítéléshez vezethet.

Az SZTFH által készített cselekvési terv minta itt érhető el:

https://sztfh.hu/tevekenysegek/kiberbiztonsagi-tanusitasok/kiberbiztonsagi-felugyelet/

pontos hivatkozás:

https://sztfh.hu/downloads/kiberbiztonsag/Cselekvesi%20terv%20minta.xlsx

4 FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 1/2025 (I.31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról