Elavult rendszerek naplózása

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/16

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.20	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A dokumentum azt vizsgálja, hogy a korlátozott naplózási képességű, saját fejlesztésű legacy rendszerek hogyan illeszthetők be a NIS2 és a hazai kiberbiztonsági szabályozás által elvárt naplózási és visszakövethetőségi keretek közé.

Amennyiben a rendszer továbbfejlesztése nem lehetséges, elfogadható a kockázatalapú megközelítés alkalmazásával kompenzáló kontrollok használata.

A jogszabályi környezet megengedi helyettesítő intézkedések bevezetését, de szigorú feltételekkel: a kontrollnak egyenértékű védelmi szintet kell nyújtania, a maradványkockázatokat formális eljárásrend szerint el kell fogadni, és az eltérést részletesen dokumentálni, vezetői szinten jóváhagyni szükséges.

Kompenzáló megoldásként elfogadható például a külső naplógyűjtés és hálózati szintű naplózás (pl. SIEM), a naplóinformációk fizikailag elkülönített, védett tárolása, a forgalom elemzése, illetve az erősen szabályozott üzemeltetési eljárások és szerepkör-alapú jogosultságkezelés. Ugyanakkor bizonyos, „Biztosító” jellegű kontrolloknál (naplózható események meghatározása, a naplóbejegyzések kötelező tartalma, a bejegyzések rendszer általi létrehozása) a rendszernek magának kell minimum szinten teljesítenie a követelményeket, ezek hiánya auditon nem fogadható el.

A legacy rendszerek cseréje vagy átalakítása hosszabb távon mindenképpen elvégzendő feladat, de rövid távon jól megtervezett kompenzáló kontroll-csomaggal, dokumentált, jóváhagyott kockázatvállalás mellett a NIS2-kompatibilis működés elérhető.

2. A VIZSGÁLANDÓ KÉRDÉS

Adott egy saját fejlesztésű, jelenleg is üzemben lévő legacy rendszer, melynek naplózási képességei jelentősen elmaradnak a modern rendszerektől. A rendszer architektúrája olyan, hogy a NIS2-ből, illetve a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényből és végrehajtási rendeleteiből következő naplózási és visszakövethetőségi követelmények teljesítése csak a rendszer magjáig lenyúló, mély fejlesztésekkel lenne megoldható. Ezek a módosítások rendkívül erőforrás-igényesek, időigényesek és technikai kockázattal járnak, ezért rövid távon nem reális a teljes körű átalakítás.

Kérdés, hogy ilyen, korlátozott naplózási funkcionalitással rendelkező legacy rendszer esetében a NIS2-nek való megfelelés során milyen mértékben és milyen feltételekkel fogadhatók el kompenzáló kontrollok (pl. külső naplógyűjtés, hálózati szintű naplózás, erősen szabályozott üzemeltetési eljárások)? Mi az az audit szempontból elvárt minimum szint a naplózásban, amit mindenképpen a rendszernek magának kell tudnia, és mely elemek válthatók ki dokumentált folyamatokkal vagy kiegészítő eszközökkel úgy, hogy az még a NIS2 szerinti megfelelőség keretein belül maradjon?

3. VÁLASZ

A Magyarország Kiberbiztonságáról szóló 2024. évi LXIX tv. (Kiberbiztonsági tv.)-nek való megfelelés során gyakran merül fel kérdésként a korlátozott naplózási képességekkel rendelkező, úgynevezett legacy rendszerek kezelése. Bizonyos esetekben megengedett a kockázatalapú megközelítés alkalmazása, amely lehetőséget biztosít kompenzáló kontrollok bevezetésére.

A 7/2024 (VI.24) MK rendelet[1] szerint amennyiben egy előírt védelmi intézkedés (kontroll) az adott technikai környezetben nem valósítható meg eredményesen vagy a kockázatokkal arányosan, a szervezet helyettesítő intézkedést alkalmazhat.

A kompenzáló kontrollok elfogadásának azonban szigorú feltételei vannak:

- Egyenértékű biztonsági képesség, amely során a helyettesítő intézkedésnek igazolhatóan olyan védelmi szintet kell nyújtania, ami egyenértékű az eredetileg előírt kontrollal, és arányos a kezelt kockázatokkal. Ez különösen kritikus szempont, ha az alapfunkciókat ellátó rendszer helyett külső megoldást vonnak be.
- Kockázat elfogadása, ami azt jelenti, hogy a szervezetnek fel kell mérnie a helyettesítő intézkedésből fakadó esetleges maradványkockázatokat, és azokat a hivatalos kockázatkezelési eljárásrendnek megfelelően el kell fogadnia.
- Dokumentálás és jóváhagyás, melynek keretében az eltérést a vonatkozó dokumentációban (4. melléklet az 1/2025. (I. 31.) SZTFH rendelethez) rögzíteni kell. Részletesen indokolni szükséges, hogy miért nem alkalmazható az eredeti intézkedés, és hogyan garantálja a helyettesítő megoldás az elvárt biztonsági szintet. Az eltéréseket minden esetben a szervezet vezetőjének vagy a kockázatvállalásra jogosult személynek kell jóváhagynia.

„Egy elektronikus információs rendszer esetén a szervezet az alábbi feltételek egyidejű fennállása esetén alkalmazhat helyettesítő intézkedést:
4.2.1. a védelmi intézkedések katalógusa nem tartalmaz az adott viszonyok között eredményesen és kockázatarányosan alkalmazható intézkedést;
4.2.2. felméri és a kockázatelemzési és kockázatkezelési eljárásrendnek megfelelően elfogadja a helyettesítő intézkedés alkalmazásával kapcsolatos kockázatot;
4.2.3. a vonatkozó dokumentumban bemutatja, hogy a helyettesítő intézkedések hogyan biztosítják az elektronikus információs rendszer egyenértékű biztonsági képességeit, biztonsági követelményszintjét, és azt, hogy miért nem használhatók a jelen rendeletben megjelölt védelmi intézkedések;
4.2.4. a helyettesítő védelmi intézkedések alkalmazását dokumentálja, és az eljárási rendnek megfelelően a szervezet vezetőjével vagy a kockázatok felvállalására jogosult szerepkört betöltő személlyel jóváhagyatja.” [7/2024. (VI. 24.) MK rendelet 1. melléklet 4.2. pont]
„1.1.3. Amennyiben a kockázatelemzés indokolja, a szervezet a 3. pontban meghatározott módon eltérhet a rendszerre vonatkozó biztonsági követelményektől,

[1] 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

illetve a 4. pont szerint alkalmazhat helyettesítő védelmi intézkedéseket." [7/2024. (VI. 24.) MK rendelet 2. melléklet 1.1.3. pont]

A gyakorlatban az alábbi megoldások fogadhatók el kompenzáló kontrollként:

- Külső naplógyűjtés és hálózati szintű naplózás, amely támogatott megközelítés. A követelmények kiemelik a naplóbejegyzések központi felülvizsgálatát és elemzését (4.16[2]), amelyet gyakran SIEM eszközökkel valósítanak meg. A szabályozás kifejezetten említi a naplóinformációk védelmét fizikailag elkülönített rendszereken történő tárolással (4.27). A hálózati forgalom elemzése (18.22, 18.29) pedig hatékonyan segítheti a rendellenességek vagy az adatszivárgás észlelését, ellensúlyozva a belső naplózás hiányosságait.
- Erősen szabályozott üzemeltetési eljárások, mivel a dokumentált folyamatok teremtik meg az elszámoltathatóság és az auditálhatóság alapjait. Bár önmagukban nem váltják ki a technikai kontrollokat, az OT rendszerek esetében – ahol gyakori a közös technikai fiókok használata – a hozzáférési jogosultságok szerepkör alapú szabályozása megfelelő kompenzációt nyújthat.

Az audit módszertana a nemzetközi gyakorlaton (NIST SP 800-53A) alapul, a hazai követelményeket pedig az 1/2025 SZTFH rendelet határozza meg. Az audit során vizsgált kontrollok közül bizonyos csoportok „Biztosító" (kritikus) besorolásúak, ami azt jelenti, hogy ezek nem zárhatók ki a vizsgálatból, és a rendszernek magának kell biztosítania azokat.

A NIS2 megfelelés keretében az alábbi naplózási képességek biztosítása kritikus:

- Naplózható események (4.2), amelynek keretében a szervezetnek meg kell határoznia a naplózandó események körét, és fel kell készítenie a rendszert azok rögzítésére. Ez az alapvető képesség (például sikeres vagy sikertelen bejelentkezések rögzítése) elengedhetetlen az utólagos kivizsgálásokhoz, ezért az audit során kizárás nélkül vizsgálandó.
- Naplóbejegyzések tartalma (4.3), amely megköveteli, hogy a bejegyzésekből pontosan megállapítható legyen az esemény típusa, ideje, helye, forrása, kimenetele és az érintett szereplők. Ez szintén „Biztosító" típusú kontroll.
- Naplóbejegyzések létrehozása (4.40), amely azt az alapvető elvárást fogalmazza meg, hogy az információs rendszer képes legyen a meghatározott eseményekről megfelelő tartalmú bejegyzéseket előállítani.

Amennyiben ezek az alapvető követelmények nem teljesülnek, az audit során az információs rendszer „nem megfelelt" minősítést kaphat.

Azok a naplózási intézkedések, amelyek technológiai korlátok miatt nehezen implementálhatók egy örökölt rendszerben, gyakran kiválthatók dokumentált folyamatokkal vagy külső

2 a () ben lévő számok a 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről 2. mellékletének követelményeire utalnak.

eszközökkel (például SIEM, loggyűjtő szerver). Ezek jellemzően a „Támogató" típusú kontrollok közé tartoznak.

Az alábbi táblázat összefoglalja azokat a naplózással kapcsolatos követelményeket, amelyeknél a kompenzációs megoldások alkalmazása elfogadott:

Követelménycsoport (MK rendelet)	**Típus**	**Kompenzációs megoldás / Funkció**
4.4. Naplóbejegyzések tartalma – Kiegészítő naplóinformációk	Támogató	Kiegészítő információk (például egyedi azonosítók) hozzárendelése a naplókhoz külső eszközzel (SIEM).
4.15. Naplózási tárhelyek összekapcsolása	Támogató	Több forrásból származó naplóadatok korrelációja és elemzése központi rendszerben.
4.23. Naplóbejegyzések csökkentése és jelentéskészítés	Támogató	A naplók automatizált feldolgozása és kereshetőségének biztosítása külső szoftverekkel.
4.27. A naplóinformációk védelme – Fizikai elkülönítés	Támogató	A naplóállományok átvitele fizikailag elkülönített, védett tárhelyre.
4.28. A naplóinformációk védelme – Kriptográfia	Támogató	A naplók sértetlenségének biztosítása utólagos titkosítással vagy aláírással a tárolóban.
4.38. A naplóbejegyzések megőrzése	Támogató	A jogszabályi megőrzési idő biztosítása dedikált archiváló rendszerrel.
4.39. Hosszú távú visszakeresési képesség	Támogató	A naplók olvashatóságának fenntartása konvertálással vagy a régi olvasóeszközök megőrzésével.

Míg a legacy rendszerek esetében a nyers adatok előállítása (az események generálása) nem megkerülhető, addig a modern elvárások szerinti elemzés, védelem és tárolás kiszervezhető külső rendszerekbe.

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény a 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