A naplózás fontossága és mélysége a NIS2 megfelelés szempontjából

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/9

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.12	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A jogszabályok részletes (és kötelező) követelményeket támasztanak az elektronikus informatikai rendszerben történt események naplózásával szemben. A jogszabályi követelmények meghatározzák a minimálisan gyűjtendő információk körét, a naplóbejegyzéseknek a jogosulatlan hozzáféréssel, módosítással és törléssel szembeni védelmét, a naplóbejegyzések felülvizsgálatával, elemzésével és az alapján teendő intézkedésekkel kapcsolatos követelményeket. Mindezeknek a követelményeknek a naplóbejegyzések szöveges (txt) fájlba történő gyűjtés nem felel meg, és komoly kockázatot jelent. Mindenképpen olyan eszközök alkalmazása indokolt, amelyek képesek biztosítani a jogszabályban meghatározott követelményeknek való megfelelést.

2. A VIZSGÁLANDÓ KÉRDÉS

Mennyire fontos a logolás az infrastruktúrában? Milyen részletekig kell eljutni? Elég ha txt-be gyűjtik az adatokat, vagy egy logelemző, riasztó rendszert kell üzemeltetni?

3. VÁLASZ

3.1 A naplózás fontossága

A naplózás nem csupán fontos, hanem alapvető jogszabályi kötelezettség. A naplózás hiánya vagy elégtelensége esetén lehetetlen a biztonsági események utólagos kivizsgálása, a felelősség megállapítása és a rendszer működésének nyomon követése.

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) előírja a szervezet vezetője számára, hogy gondoskodjon az események nyomonkövethetőségéről. Ez az alapvető követelmény minden érintett szervezetre vonatkozik.

> *„(5) A szervezet vezetője az elektronikus információs rendszer védelmének biztosítása érdekében [...] c) gondoskodik az elektronikus információs rendszer eseményeinek nyomonkövethetőségéről;" [2024. évi LXIX. törvény 6. § (5) bekezdés c) pont]*

3.2 A naplózás mélysége és tartalma

A naplózás mélysége és tartalma tekintetében a 7/2024. (VI. 24.) MK rendelet (továbbiakban: MK rendelet) részletesen meghatározza, hogy milyen adatokat kell rögzíteni. Nem elegendő puszta hibakódokat tárolni; a naplóbejegyzéseknek alkalmasnak kell lenniük a "ki, mit, mikor, hol és hogyan" kérdések megválaszolására.

A naplózásnak ki kell terjednie a sikeres és sikertelen eseményekre, a hozzáférésekre, a jogosultságok változására és a rendszerhibákra. A jogszabály konkrétan meghatározza a

naplóbejegyzések kötelező minimális tartalmát minden biztonsági osztály (Alap, Jelentős, Magas) esetében.

> *„4.3. A szervezet biztosítja, hogy a naplóbejegyzésekből az alábbi információk megállapíthatóak legyenek: 4.3.1. milyen típusú esemény történt; 4.3.2. mikor történt az esemény; 4.3.3. hol történt az esemény; 4.3.4. miből származott az esemény; és 4.3.5. mi volt az eseménynek a kimenetele, valamint 4.3.6. az eseményhez kapcsolódó személyek, alanyok, objektumok." [7/2024. (VI. 24.) MK rendelet 2. melléklet 4.3. pont]*

A pontosság érdekében az időbélyegek használata is kötelező, amelynek szinkronizáltnak kell lennie (NTP).

> *„4.24. A szervezet: [...] 4.24.2. Időbélyegeket rögzít a naplóbejegyzésekben, amelyek megfelelnek a szervezet által meghatározott pontosságra vonatkozó követelményeknek, a koordinált világidőt használják és magukba foglalják a helyi időeltolódást." [7/2024. (VI. 24.) MK rendelet 2. melléklet 4.24. pont]*

3.3 TXT fájlok gyűjtése vagy logelemző rendszer?

A kérdés kritikus pontja a technikai megvalósítás. Bár az „Alap” biztonsági osztályban elméletileg elképzelhető lenne egyszerűbb megoldás, a puszta szöveges (txt) fájlba történő gyűjtés önmagában nem elegendő, és komoly kockázatot jelent, különösen a „Jelentős” és „Magas” biztonsági osztályokban. Ennek okai:

- Manipulálhatóság: A sima szöveges fájlok könnyen módosíthatók vagy törölhetők a támadók (vagy belső elkövetők) által a nyomok eltüntetése érdekében. A jogszabály előírja a naplóinformációk védelmét a jogosulatlan hozzáféréssel és módosítással szemben.
- Elemzés hiánya: A jogszabály előírja a naplók rendszeres felülvizsgálatát és elemzését [4.13-4.21. követelmények, számos opcionális]. Több száz gigabájtnyi txt fájlt manuálisan lehetetlen hatékonyan elemezni.
- Automatizáltság: A magasabb biztonsági osztályokban kifejezett elvárás az automatizált feldolgozás és a valós idejű riasztás.

Az MK rendelet előírásai alapján a központosított naplógyűjtés és elemzés (SIEM rendszerek vagy ahhoz hasonló megoldások) bevezetése erősen ajánlott, magasabb osztályokban pedig elengedhetetlen.

A naplók védelme:

> *„4.25. Az EIR: 4.25.1. Megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben."*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 4.25. pont]*

3.4 Automatizált feldolgozás és kereshetőség:

Különösen a „Jelentős” és „Magas” biztonsági osztályokban az MK rendelet előírja, hogy a naplók legyenek automatikusan feldolgozhatók és kereshetők. Ez txt fájlokkal nehezen vagy egyáltalán nem teljesíthető hatékonyan.

> *„4.23. A szervezet gondoskodik arról, hogy a naplóbejegyzések automatikusan feldolgozhatók, rendezhetők és kereshetők legyenek a meghatározott adatmezők tekintetében." [7/2024. (VI. 24.) MK rendelet 2. melléklet 4.23. pont]*

Nem elég gyűjteni az adatokat, a kritikus hibákról (pl. naplózási hiba, tárhely betelte) riasztást is kell küldeni.

> *„4.9. Az EIR riasztást küld a meghatározott személyeknek vagy szerepköröknek, ha a meghatározott, valós idejű riasztást igénylő hibaesemények közül bármelyik bekövetkezik." [7/2024. (VI. 24.) MK rendelet 2. melléklet 4.9. pont]*

A puszta txt-be gyűjtés a legtöbb esetben nem elégséges, és nem felel meg a modern kiberbiztonsági követelményeknek, különösen a jogszabályi megfelelőség szempontjából.

Javasolt intézkedések:

- Központosított naplógyűjtés, dedikált log-szerver vagy SIEM (Security Information and Event Management) rendszer használata.
- Sértetlenségvédelem: annak biztosítása, hogy a naplókhoz senki ne férjen hozzá módosítási joggal (pl. WORM - Write Once Read Many tárolók, vagy digitális aláírás).
- Elemzés és riasztás: automatikus elemzések és riasztások konfigurálása a kritikus eseményekre (pl. sikertelen belépési sorozatok, privilegizált fiókok használata, malware észlelése).

Az infrastruktúra méretétől és a rendszer biztonsági osztályától függően (amelyet a hatáselemzés alapján kell meghatározni) kell kiválasztani a megfelelő eszközt, de az automatizált elemzés és a védett tárolás minden esetben kritérium.

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