"Alap" biztonsági osztályban szükséges e IPS/IDS és SOC üzemeltetése?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/7

VERZIÓKÖVETÉS

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

1. VEZETŐI ÖSSZEFOGLALÓ

Az Alap biztonsági osztályba sorolt rendszerek esetében a magyar kiberbiztonsági szabályozás nem írja elő sem dedikált biztonsági műveleti központ (SOC), sem önálló, speciális hardverre vagy szoftverre épülő IDS/IPS rendszer kötelező üzemeltetését.

Mindemellett egyértelműen kötelezettség a biztonsági események arányos, kockázatalapú kezelése és a rendszerek rendszeres monitorozása. A naplózásnak ki kell terjednie a kritikus rendszerelemekre (például szerverek, tűzfalak, központi hálózati eszközök) és a biztonsági szempontból releváns eseményekre (sikertelen bejelentkezések, adminisztrátori műveletek, jogosultság-módosítások), de nem szükséges minden végfelhasználói munkaállomás minden eseményét rögzíteni, ha az nem indokolt a kockázatok alapján.

A jogszabály az arányosság elvét követi, a cél az incidensek utólagos visszakövethetőségének biztosítása, nem a teljes körű megfigyelés, ezért a szervezetnek belső szabályzatban kell meghatároznia, mit naplóz, milyen mélységben és milyen gyakorisággal vizsgálja ezeket, jellemzően az általános IT üzemeltetés keretei között

2. A VIZSGÁLANDÓ KÉRDÉS

„Alap” biztonsági osztályba tartozó EIR esetén Kötelező-e SoC-t (biztonsági műveleti központ – Security Operations Center) üzemeltetni? IPS/IDS kötelező-e? Minden IT eszközről kell naplókat gyűjteni/elemezni?

3. VÁLASZ

A 7/2024. (VI. 24.) MK rendelet (a továbbiakban: MK rendelet) alapján az „Alap” biztonsági osztályba sorolt elektronikus információs rendszerek (EIR) esetében a követelmények enyhébbek, mint a „Jelentős” vagy „Magas” osztályoknál.

Alap szinten nem kell minden eszközről minden eseményt naplózni, és nem kötelező a dedikált Biztonsági Műveleti Központ (SOC) üzemeltetése sem, de az eseménykezelés minimális követelményit teljesíteni kell.

3.1 Naplózás

Az MK rendelet az arányosság elvét követi. Alap szinten a cél a „nyomonkövethetőség” biztosítása, nem a totális megfigyelés.

Az Alap biztonsági osztályban kötelező a naplózási követelmények teljesítése, de a szervezetnek van mozgástere abban, hogy pontosan mely eseményeket naplózza. A jogszabály előírja, hogy a szervezetnek meg kell határoznia a naplózandó eseményeket az EIR-en belül.

Miről kötelező naplót gyűjteni?

- A kritikus rendszerelemekről (pl. szerverek, tűzfalak, központi hálózati eszközök).

- A biztonsági szempontból releváns eseményekről (pl. sikertelen bejelentkezések, adminisztrátori tevékenységek, jelszóváltoztatások, jogosultságok módosítása).

Miről nem kötelező naplót gyűjteni (általában)?

- Végfelhasználói munkaállomások (PC-k, laptopok) minden egyes kattintásáról vagy irreleváns rendszerüzenetéről, kivéve, ha azok kritikus adatot kezelnek.
- Perifériákról (pl. nyomtatók, kivéve ha hálózatiak és adminisztrálhatók), "buta" switch-ekről.

Az elvárás, hogy a naplók tartalmának elegendőnek kell lenniük ahhoz, hogy egy esetleges incidens (pl. betörés) utólag rekonstruálható legyen. Ehhez az MK rendelet meghatározza a naplóbejegyzések minimális tartalmát.

A vonatkozó előírások az MK rendelet 2. mellékletéből:

- A naplózható események meghatározása:

  "4.2. A szervezet: 4.2.1. Meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az EIR-t. [...] 4.2.3. Meghatározza az EIR-en belül naplózandó eseménytípusokat, és az azokhoz kapcsolódó gyakoriságot vagy az azt szükségessé tevő eseményeket." [7/2024. (VI. 24.) MK rendelet 2. melléklet 4.2. pont (A)]

- A naplóbejegyzések minimális tartalma:

  „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)]

- A naplóbejegyzések felülvizsgálata:

  "4.13. A szervezet: 4.13.1. Meghatározott gyakorisággal felülvizsgálja és elemzi a rendszer naplóbejegyzéseit a nem megfelelő vagy szokatlan tevékenységre utaló jelek és az ilyen tevékenységek lehetséges hatásai szempontjából." [7/2024. (VI. 24.) MK rendelet 2. melléklet 4.13. pont (A)]

3.2 Kötelező-e SOC-t (Security Operations Center) üzemeltetni?

Az Alap biztonsági osztályban nem kötelező önálló Biztonsági Műveleti Központ (SOC) létrehozása és fenntartása.

A "SOC" egy folyamatos (gyakran 24/7) monitorozást végző központot jelent, ami jellemzően a kiemelt kockázatú szervezetek elvárása.

Mi az, ami viszont kötelező?

- Biztonsági események kezelése, a szervezetnek rendelkeznie kell egy szabályozott folyamata arra, mi történik, ha kiberbiztonsági probléma merül fel van (ki(k) köteleset eljárni, ki(k)nek és hogyan kell jelenteni az eseményeket).
- Monitorozás, ez nem jelent folyamatos, 24 órás élőerős figyelést, de a rendszerek állapotát és a naplókat rendszeresen (pl. hetente vagy riasztás esetén) ellenőrizni kell.

Alap szinten ezt gyakran a meglévő IT üzemeltetés végzi, nem egy külön biztonsági csapat.

A vonatkozó követelménycsoport (9.23) az MK rendelet alapján kiegészítő intézkedésnek minősül, opcionális elvárásként jelenik meg.

> *"9.23. A szervezet létrehoz és fenntart egy biztonsági műveleti központot." [7/2024. (VI. 24.) MK rendelet 2. melléklet 9.23. pont (Opcionális követelmény)]*

Ugyanakkor a biztonsági események kezelése általánosságban kötelező:

> *"9.9.1. A szervezet: 9.9.2. Biztonsági eseménykezelési képességet alakít ki, amely összhangban van a biztonsági eseménykezelési tervvel, és magában foglalja a felkészülést, az észlelést és elemzést, az elszigetelést, a felszámolást és a helyreállítást." [7/2024. (VI. 24.) MK rendelet 2. melléklet 9.9. pont (A)]*

3.3 IPS / IDS (behatolásjelző/megelőző rendszer) kötelező-e?

Különálló, dedikált behatolásérzékelő rendszer (IDS) üzemeltetése nem kötelező (opcionális/kiegészítő) az Alap biztonsági osztályban, de a rendszer monitorozása (figyelése) általánosságban elvárt.

A jogszabály különbséget tesz fizikai és logikai védelem között:

A szervezet helyiségeibe (különösen a szerverszobába/adatközpontba) való behatolás érzékelése (fizikai védelem) alap szinten is elvárt (pl. beléptetőrendszer, riasztó alkalmazása), hálózati szinten viszont általában nem kötelező, de erősen ajánlott a határvédelmen.

Alap szinten, a határvédelmi eszközökön (tűzfal) lévő alapvető szűrés és a gyanús forgalom blokkolása az elvárás. Nem kötelező különálló, dedikált IDS/IPS célhardver beszerzése, ha a tűzfal rendelkezik ilyen alapfunkciókkal (pl. beépített IPS modul).

A hangsúly a határvédelmen van a belső hálózat minden szegmensének IDS monitorozása alap szinten nem elvárás.

Behatolásérzékelő rendszer (IDS), kiegészítő intézkedés:

> *"18.14. A szervezet az egyedi behatolásérzékelő eszközöket egy rendszerszintű behatolásérzékelő rendszerbe konfigurálja és csatlakoztatja." [7/2024. (VI. 24.) MK rendelet 2. melléklet 18.14. pont (A: -, J: -, M: -)] .*

Valós idejű elemző eszközök alkalmazása csak Jelentős és Magas szinten kötelező:

> *"18.15. Az EIR automatizált eszközöket és mechanizmusokat alkalmaz, amelyek támogatják az események majdnem valós idejű elemzését." [7/2024. (VI. 24.) MK rendelet 2. melléklet 18.15. pont (A: -, J: X, M: X)]*

Általános monitorozás (ami Alap szinten is kötelező):

> *"18.13. A szervezet: 18.13.1. Monitorozza a rendszert, hogy észlelje: 18.13.1.1. A támadásokat és a potenciális támadásokra utaló jeleket összhangban a meghatározott felügyeleti célokkal;" [7/2024. (VI. 24.) MK rendelet 2. melléklet 18.13. pont (A)]*

Alap szinten a támadások észlelésére szolgáló monitorozás (18.13) kötelező, de ez nem írja elő specifikusan dedikált IDS/IPS hardver vagy szoftver (18.14) vagy automatizált valós idejű elemző eszközök (18.15) használatát; ezeket egyszerűbb eszközökkel (pl. tűzfal naplók elemzése, alapvető hoszt-alapú védelem) is meg lehet valósítani

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