„Alap” biztonsági osztályban mi az elfogadott tűzfal technológia és konfiguráció?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/8

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.30	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A jogszabály nem írja elő, hogy a határvédelmi eszköznek (tűzfalnak) dedikált, kizárólag erre a célra gyártott céleszköznek kell lennie. A követelmény a funkcionalitásra vonatkozik: az eszköznek képesnek kell lennie a határok védelmére, a kommunikáció ellenőrzésére és a forgalom szabályozására, szűrésére. A PC-n és mobil eszközön központilag felügyelt tűzfal- és vírusirtó szoftvert használata jó gyakorlat, de nem váltja ki a hálózati határvédelmet.

2. A VIZSGÁLANDÓ KÉRDÉS

Tűzfal tekintetében mi az elfogadható technológiai szint „alap” besorolásnál? Szükséges-e külön célhardver (pl Mikrotik) vagy elegendő egy megfelelően konfigurált szoftveres eszköz? Elfogadható-e az, ha minden PC-n, mobil eszközön használunk központilag felügyelt/kezelt tűzfal-vírusírtó szoftvert?

3. VÁLASZ

3.1 A kérdésben szereplő megoldás megfelelősége

A javasolt megoldás, azaz a Mikrotik router a hálózati határon és központilag menedzselt végponti védelem megfelel az „Alap” biztonsági osztály követelményeinek, amennyiben:

- A határvédelmi eszközön beállítják a szigorú tűzfalszabályokat (kívülről minden tiltva, kivéve, ami üzletileg indokolt).
- A végponti szoftverek (host-based protection) minden eszközön aktívak.
- A határvédelmi eszköz szoftverét rendszeresen frissítik a 7/2024 (VI.24) MK rendelet 18.6. pont (Hibajavítás – Automatikus szoftver és firmware frissítés) előírásainak megfelelően.

Az „Alap” biztonsági osztályba sorolt elektronikus információs rendszerek esetében a jogszabály kötelezően előírja a hálózati határok védelmét, azaz a határvédelmi eszközök alkalmazását. Ez azt jelenti, hogy nem elegendő kizárólag a végpontokon (PC-k, mobilok) futó szoftveres védelem, hanem a hálózati belépési ponton is szükséges védelmi intézkedés.

A vonatkozó követelmények a 7/2024 (VI.24) MK rendelet 2. mellékletéből:

> *„17.17. A határok védelme*
> *17.17. A szervezet:*
> *17.17.1. Ellenőrzi a kommunikációt a menedzselt külső interfészein, valamint a rendszer kulcsfontosságú menedzselt belső interfészein. [...]*
> *17.17.3. Csak a szervezet biztonsági architektúrájával összhangban lévő határvédelmi eszközökön keresztül, menedzselt interfészek segítségével kapcsolódik külső hálózatokhoz vagy külső EIR-ekhez.”*

Továbbá az „Alap” szinten is kötelező az alapértelmezett tiltás elvének alkalmazása a hálózati forgalomra:

> *„17.20. A határok védelme – Alapértelmezés szerinti elutasítás és kivétel alapú engedélyezés*
> *17.20. Az EIR alapértelmezés szerint elutasítja a hálózati kommunikációs forgalmat, és csak kivételként engedélyezi azt a menedzselt interfészeknél.”*

3.2 Megfelelő-e egy tűzfal funkcionalitással rendelkező router vagy kell külön hardver?

A jogszabály nem írja elő, hogy a határvédelmi eszköznek (tűzfalnak) dedikált, kizárólag erre a célra gyártott céleszköznek (pl. célhardveres Next-Generation Firewallnak) kell lennie. A követelmény a funkcionalitásra vonatkozik: az eszköznek képesnek kell lennie a határok védelmére, a kommunikáció ellenőrzésére és a forgalom szabályozására (szűrésére).

Ezért a válasz a kérdésére:

- Nem szükséges külön, dedikált hardveres tűzfal célhardver beszerzése, amennyiben a meglévő hálózati eszköz (router) rendelkezik tűzfal funkciókkal.
- Elegendő egy megfelelően konfigurált eszköz, például egy Mikrotik router, amennyiben az képes ellátni a fenti jogszabályi funkciókat (csomagszűrés, forgalomirányítás, naplózás).

Fontos feltétel, hogy a határvédelmi eszköz önmagában csak akkor felel meg, ha megfelelően van konfigurálva. Ez az „Alap” szinten azt jelenti, hogy:

- alapértelmezetten tiltja a bejövő forgalmat (lásd 17.20. pont),
- csak a szükséges portokat és szolgáltatásokat engedélyezi,
- a menedzsment felületek (pl. Winbox, SSH) nem érhetők el a nyilvános internet felől korlátozás nélkül.

3.3 A végponti védelem (szoftveres tűzfal/vírusirtó) szerepe

Az, hogy minden PC-n és mobil eszközön központilag felügyelt tűzfal- és vírusirtó szoftvert használnak, jó gyakorlat és megfelel más jogszabályi követelményeknek, de nem váltja ki a hálózati határvédelmet.

A végponti védelem az alábbi követelményeket teljesíti, amelyek szintén kötelezőek „Alap” szinten:

> *„17.26. A határok védelme – Hosztalapú védelem*
> *17.26. A szervezet az általa meghatározott hosztalapú határvédelmi mechanizmusokat megvalósítja a meghatározott rendszerelemeken.”*

A végponti védelemnek teljesítenie kell továbbá a kártékony kódok elleni védelmet is:

> *„18.8. Kártékony kódok elleni védelem*
> *18.8. A szervezet:*

18.8.1. Kártékony kódok elleni védelmi mechanizmusokat alkalmaz a rendszer belépési és kilépési pontjain [...]
18.8.3. A kártékony kódok elleni védelmi mechanizmusokat úgy konfigurálja, hogy:
18.8.3.1. Meghatározott időközönként átvizsgálja a rendszert, és valós időben ellenőrzi a külső forrásokból származó fájlokat a végpontokon [...]"

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