Fizikai védelmi intézkedések alkalmazása elektronikus adattárolása nem használt telephely esetében

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/10

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.30	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió
1.1	2027.02.13	Kálmán és Társai Ügyvédi Iroda	Stilisztikai javítások

1. VEZETŐI ÖSSZEFOGLALÓ

Felhő alapú működés mellett (home office) a klasszikus „szervertermi" fizikai követelmények jelentős része jogszerűen mellőzhető, ha az irodában nincs szerver és kritikus adathordozó, és ezt kockázatelemzés, valamint eltérésnyilvántartás támasztja alá. A 7/2024. (VI. 24.) MK rendelet alapján a fizikai védelmi intézkedéseket csak azokra a létesítményekre kell alkalmazni, amelyek közvetlenül védelmet nyújtanak az EIR számára; az iroda ilyenkor adminisztratív tér, ahol elegendő az alapvető hozzáférés-korlátozás és a munkaállomások, papíralapú iratok védelme. A fizikai biztonság súlypontja a felhőszolgáltató adatközpontjára és a végpontokra kerül, amelyet tanúsítványokkal (pl. ISO 27001, SOC 2) és szerződéses kötelezettségekkel kell igazolni, valamint a „megosztott felelősségi modellben" dokumentálni. Távmunka esetén az alternatív munkavégzési helyekre, mobil eszközökre vonatkozó szabályok, a teljes lemeztitkosítás, a biztonságos kapcsolatok (VPN), a végpontvédelmi riportok és a munkavállalók oktatása jelentik a fő kontrollokat; az audit fókusza így nem az irodaépületre, hanem a felhő- és végpontvédelem bizonyítékaira helyeződik.

2. A VIZSGÁLANDÓ KÉRDÉS

Adott egy cég, amelynek működése alapvetően nem függ az irodától, a kollégák nagy része távolról dolgozik, az alkalmazásaink adatközpontokban, részben felhőben futnak. Ilyen esetekben hogyan kell kezelni a fizikai biztonságra vonatkozó elvárásokat?

3. VÁLASZ

A hatályos szabályozás (különösen a 7/2024. (VI. 24.) MK rendelet) előírja a megfelelő fizikai és környezeti védelmi intézkedések megtételét, azonban a jogalkotó ismeri, hogy pl. a modern technológiai környezet (felhő, home office) sajátosságai miatt eltérések lehetnek indokoltak. A biztonsági osztályhoz tartozó védelmi intézkedések meghatározásakor „az elektronikus információs rendszerre értelmezendő és alkalmazandó biztonsági követelményeket" kell meghatározni. Egy audit során nem azt kell bizonyítani, hogy van egy üres irodában beléptetőrendszer, hanem azt, hogy az adatok és a rendszerek ott vannak védve, ahol ténylegesen elhelyezkednek (felhő, végpontok).

A 7/2024. (VI. 24.) MK rendelet által előírtaktól eltérni az elvégzendő kockázatelemzés alapján lehet. A jogszabály kifejezetten lehetővé teszi az eltérések alkalmazását, amennyiben a fizikai infrastruktúra nem releváns az elektronikus információs rendszer (EIR) védelme szempontjából.

Ha – a kérdésfeltevésben írtak szerint - a szervezet székhelyén/telephelyén nem található szerver, és nem tárolnak kritikus adathordozót, akkor a fizikai védelmi intézkedések jelentős része az adott helyszínen nem releváns vagy egyszerűsített módon alkalmazandó. Erre a 7/2024. (VI. 24.) MK rendelet kifejezett felmentést ad az "eltérések" fejezetben.

3.2.2.1. A szervezeti létesítményekkel kapcsolatos védelmi intézkedések csak azokra a létesítményekre alkalmazandók, amelyek közvetlenül nyújtanak védelmet vagy biztonsági támogatást az elektronikus információs rendszernek, vagy kapcsolatosak azzal. [7/2024. (VI. 24.) MK rendelet 1. melléklet 3.2.2.1. pont]

A szervezet teendői:

- a "Eltérések és helyettesítő védelmi intézkedések nyilvántartásában" (1/2025. SZTFH rendelet 4. melléklet) rögzíteni kell, ha az adott helyiség nem része az EIR fizikai határának, mert nem tárol adatot/eszközt, ezért a szervertermekre vonatkozó előírások (pl. tűzoltórendszer, szünetmentes táp a szervereknek) ott nem alkalmazhatók.
- továbbra is releváns marad pl. a belépés fizikai korlátozása (zárt ajtó), hogy illetéktelenek ne férhessenek hozzá az ott hagyott munkaállomásokhoz vagy papíralapú dokumentumokhoz; vagy a munkaállomások védelmére vonatkozó előírások.

Amennyiben az alkalmazások felhőszolgáltatóknál találhatók, a fizikai biztonság követelményei ide összpontosulnak. Mivel azonban ezt a feladatot a szervezet kiszervezte, a fizikai védelemről a szolgáltatónak kell gondoskodnia, a szervezetnek pedig ezt ellenőriznie kell.

16.49.1. A szervezet szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett EIR-ek szolgáltatásai megfeleljenek a szervezet elektronikus információbiztonsági követelményeinek, és a szervezet által meghatározott védelmi intézkedéseket alkalmazzák.
16.49.3. A szervezet külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső EIR szolgáltatója megfelel-e az elvárt védelmi intézkedéseknek. [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.49. pont]

Audit során bizonyítékul szolgálhatnak:

- a felhőszolgáltató/adatközpont érvényes tanúsítványai (pl. ISO 27001, SOC 2 Type II), amelyek igazolják a fizikai védelmet,
- a "megosztott felelősségi modell" dokumentálása a Rendszerbiztonsági Tervben.

A távmunka/otthoni munkavégzés (home office) esetében a munkavállalók tthona vagy más tartózkodási helye a munkavégzés helye, ahonnan a saját internetkapcsolatukon (esetleg más szervezet internetkapcsolatán) keresztül kapcsolódnak a szervezet szervereihez, alkalmazásaihoz. A munkaállomások (a szervezet által biztosított eszközök) használatának korlátozására (pl. folyamatos fizikai felügyelet alatt tartására, egyes helyeken való használatának korlátozására/kizárására) vonatkozó szabályokon túl védelem súlypontja áthelyeződik a logikai védelemre (titkosítás), a jogosultságok, hitelesítések, biztonságos kapcsolatok (például VPN) kialakítására, a rendszeres mentésekre stb.

A 7/2024. (VI. 24.) MK rendeletnek az „alternatív munkavégzési helyekre” vonatkozó szabályai alkalmazhatóak lehetnek a jelzett helyzetekre:

12.43. A szervezet:
12.43.1. meghatározza és dokumentálja az alternatív munkavégzési helyeket a munkavállalók számára;

> *12.43.2. meghatározza a védelmi intézkedéseket az alternatív munkavégzési helyeken; [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.43. pont]*

Ezen felül alkalmazni lehet a mobil eszközökre vonatkozó előírást is:

> *2.114. A szervezet teljes eszköztitkosítást vagy tárolóalapú titkosítást alkalmaz a meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének védelme érdekében.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 2.114. pont]*

Az auditor számára az alábbi dokumentumokat és bizonyítékokat kell előkészíteni a fizikai biztonság igazolására ebben a speciális környezetben:

1. Eltérések és helyettesítő intézkedések nyilvántartása
   - Ebben kell rögzíteni, hogy a fizikai iroda nem tárol éles adatot, ezért a szervertermi követelmények (klíma, oltórendszer) "Nem alkalmazható" státuszúak. Indoklás: Az infrastruktúra felhő alapú.
2. Rendszerbiztonsági terv
   - Pontosan definiálni kell az EIR határait. A határ a felhőszolgáltató interfésze és a munkavállalói eszközök (laptopok).
   - Rögzíteni kell a felhőszolgáltatóval kapcsolatos felelősségmegosztást.
3. Beszállítói menedzsment bizonyítékok
   - Beszállítói kockázetelemzés
   - A felhőszolgáltató (AWS, Azure, Google, stb.) és az adatközpont érvényes biztonsági tanúsítványainak letöltött példányai.
   - A szolgáltatási szerződések (SLA), amelyek hivatkoznak a biztonsági megfelelőségre.
4. A távmunkára vonatkozó szabályozás és oktatás
   - Szabályzat, amely előírja a "tiszta asztal elvét" otthoni környezetben is.
   - Előírás a képernyőzár használatára és arra, hogy illetéktelen (családtag) nem tekintheti meg a monitort.
   - Bizonyíték, hogy a dolgozók ezt a szabályzatot megismerték.
5. Végpontvédelmi riportok
   - Mivel a fizikai eszköz (laptop) bárhol lehet, a bizonyíték a lemez-titkosítás (pl. BitLocker, FileVault) megléte.
   - Központi riport arról, hogy minden céges eszköz titkosított. Ez a "helyettesítő kontroll" a fizikai elzárás helyett.

Jelen esetben a fizikai biztonsági audit nem az irodaépület falainak vizsgálatáról szól, hanem a bizalom láncolatáról és az eszközök logikai védelméről.

Az auditor felé a következő érvelést kell felépíteni:

- Az iroda nem minősül az EIR kritikus üzemeltetési környezetének (csak adminisztráció), ezért a 7/2024 MK rendelet 1. melléklet 3.2.2.1. pontja alapján a szigorú fizikai követelmények alól mentesül.

- A fizikai védelmet a felhőszolgáltató biztosítja (bizonyíték: pl ISO/SOC2 tanúsítványok).
- A végpontok fizikai elvesztése elleni védelmet a teljes lemeztitkosítás és a távoli törlés képessége biztosítja (bizonyíték: MDM riport).

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. SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról