

Elhagyható-e a szerverszoba?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/34

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.23	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

Sem a Kiberbiztonsági tv., sem a 7/2024. (VI. 24.) MK rendelet nem írja elő, hogy a szervezetnek szerverszobával kell rendelkeznie. A „szerver szoba” kifejezés a rendelet teljes szövegében egyetlen helyen, a környezeti védelmi intézkedések között szerepel, ott is csak példaként az informatikai erőforrásokat koncentráltan tartalmazó helyiségekre. A rendelet nem helyiségtípust, hanem védelmi eredményt követel meg. Azt írja elő, hogy az elektronikus információs rendszernek helyet adó létesítménybe csak az arra jogosultak léphessenek be, a belépés ellenőrzött és naplózott legyen, a rendszerelemeket tartalmazó helyiségek a szervezet ellenőrzése alatt álljanak, és a berendezéseket tűz, víz, áramkimaradás és kedvezőtlen környezeti feltételek ellen védjék.

Ebből következik, hogy a jogszabályoknak szerverszoba nélkül is meg lehet felelni. Alap és jelentős biztonsági osztályban a szerverek és a hálózati eszközök irodai vagy üzemi helyiségben is elhelyezhetők, ha a helyiség vagy az abban elhelyezett zárható rackszekrény teljesíti a fizikai és környezeti védelem követelményeit. Ez azonban a megengedett minimum, nem a javasolt megoldás. Ha a szervezet saját infrastruktúráján üzemeltet rendszereket, a külön szerverszoba kialakítását már alap biztonsági osztályban is kiemelten ajánljuk. Az irodai elhelyezésnél ugyanis

az a helyiség, ahol a szerver áll, a rendelet szemszögéből informatikai erőforrásokat koncentráltan tartalmazó helyiséggé válik. Ott a hőmérsékletet és a páratartalmat felügyelni kell, tűzérzékelést kell biztosítani, a belépési rendet és a kulcsokat ugyanúgy kezelni kell, mint egy gépteremben, és minden eltérést kockázatelemzéssel kell alátámasztani. Egy közös használatú irodában ez sokkal bonyolultabb és költségesebb, mint egy kis, zárható, klimatizált helyiség, amelyben ugyanezek a követelmények szinte maguktól teljesülnek. Jelentős osztályban a szünetmentes áramellátás, a kábelezés és a rendszerelosztók védelme, valamint a behatolásjelzés követelménye ezt a különbséget tovább növeli.

Magas biztonsági osztályban a rendelet a rendszerelemeket tartalmazó helyiségekbe történő belépést a létesítménybe történő belépéstől független, külön engedélyhez köti, és a rendszerelemek elhelyezésénél a jogosulatlan hozzáférés lehetőségének minimalizálását kívánja meg. Ez egy közös használatú irodában nem teljesíthető. Magas osztályban ezért a szervereknek és a központi hálózati eszközöknek külön zárt, csak külön engedéllyel megközelíthető helyiségben kell lenniük. Ez funkcionálisan szerverszoba, még ha csak néhány négyzetméter is.

A felhőszolgáltatások igénybevétele nem szünteti meg a fizikai védelmi kötelezettségeket, csak áthelyezi a súlypontjukat. A szolgáltatónál működő rendszerelemek fizikai védelmét a szervezet szerződéses kötelemként érvényesíti, a telephelyén maradó hálózati eszközök és végpontok védelméért azonban maga felel. Egy kizárólag felhőt használó szervezetnek tehát nem kell szerverszoba, de zárható hálózati szekrényre, kulcskezelésre és belépés-ellenőrzésre szüksége van. A részben helyi rendszereket üzemeltető szervezet kötelezettsége pedig nem a szerverszoba megépítése, hanem az, hogy a biztonsági osztály szerinti követelményeket a választott elhelyezésre bizonyíthatóan teljesítse. Ehhez a legegyszerűbb és hosszabb távon a legolcsóbb út a külön szerverszoba.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2¹-kötelezett szervezet (a továbbiakban mint „Szervezet”) a fizikai védelmi szabályzatának kidolgozása és a rendszerbiztonsági terv összeállítása során azzal a kérdéssel szembesül, hogy a jogszabályok megkövetelik-e külön szerverszoba kialakítását. A Szervezet üzleti alkalmazásainak egy részét felhőszolgáltatásként veszi igénybe, telephelyén ugyanakkor továbbra is működnek helyi szerverek, hálózati és adatmentő eszközök, jelenleg egy irodai helyiség sarkában, illetve egy üzemi helyiségben elhelyezett szekrényben.

A vizsgálandó kérdés kettős. Ha a Szervezet nem kizárólag felhőszolgáltatásokat használ, mindenképpen szükség van-e szerverszobára? Tárolhatók-e a szerverek és a hálózati eszközök irodai vagy üzemi helyiségben, vagy a jogszabály külön szerverszobát követel meg? Az állásfoglalás azt is vizsgálja, hogy a válasz hogyan függ a biztonsági osztálytól, és mi a helyzet a kizárólag felhőt használó szervezeteknél.

Nem tárgya az állásfoglalásnak a szerverszobák építészeti, tűzvédelmi és villamos méretezése.

¹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályaon kívül helyezéséről (NIS 2 irányelv)

3. GYAKORLATI JAVASLATOK

3.1 Döntési szempontok a biztonsági osztály szerint

A szerverek és a hálózati eszközök elhelyezéséről a Szervezet a biztonsági osztályba sorolás eredménye és a kockázatelemzés alapján dönt. A döntést a rendszerbiztonsági tervben dokumentálja, amelynek minden osztályban tartalmaznia kell az EIR működési környezetét.² Saját infrastruktúra esetén már alap osztályban is a külön helyiséget javasoljuk, az alábbi szempontok azt mutatják, mikor fogadható el ettől eltérés.

- a) Alap osztályban az irodai vagy üzemi elhelyezés elfogadható, ha a helyiség ajtaja zárható, a belépésre jogosultak listája a helyiségre is értelmezhető, az eszközök zárható rackszekrényben vannak, a helyiségben van tűzérzékelő, a hőmérsékletet mérik, és a szekrény nem vízvezeték vagy beázásra hajlamos tető alatt áll. Javaslatunk ugyanakkor már itt is a különálló szerverszoba, mert ezek a feltételek egy erre a célra kialakított helyiségben egyszerűbben és olcsóbban tarthatók fenn.
- b) Jelentős osztályban az irodai elhelyezés még lehetséges, de már csak akkor, ha szünetmentes áramellátás, vészkipcsolási lehetőség, a kábelezés és a rendszerelosztók zárt védelme, valamint a létesítmény belépési pontjain behatoláslétesítő is működik. Ebben az osztályban a különálló szerverszobát már nem csak javasoljuk, hanem az egyetlen gazdaságos megoldásnak tartjuk, mert az irodai elhelyezés hiányosságainak dokumentált kompenzálása rendszerint többbe kerül, mint egy kis, zárható helyiség kialakítása.
- c) Magas osztályban a rendszerelemek csak külön engedéllyel megközelíthető, a többi helyiségtől elkülönített térben helyezhetők el. Ez lehet kis szerverszoba vagy adatközponti kolokáció. A közös használatú iroda nem felel meg.
- d) Kizárólag felhőt használó szervezetnél a helyi hálózati eszközök (tűzfal, kapcsoló, hozzáférési pontok) zárható hálózati szekrényben helyezhetők el, az eszközök helyét és a szekrény kulcsát kezelő eljárással. Külön szerverszoba nem szükséges, a szekrényt azonban itt is nem irodai célú, zárható technikai helyiségben érdemes elhelyezni.

3.2 Az irodai elhelyezés minimális feltételei

Ha a Szervezet a javaslatunk ellenére az alap vagy a jelentős osztályba tartozó rendszerelemeit irodai vagy üzemi helyiségben helyezi el, a rendelet követelményeit erre a helyiségre kell teljesítenie. Az alábbi megoldások ezt a helyzetet kezelik, és egyben megmutatják, mennyi külön intézkedést tesz szükségtelenné (vált ki) egyetlen különálló szerverszoba.

A zárható rackszekrény a legfontosabb elem. A rendelet a zárható házat opcionális intézkedésként nevesíti, a NIST forráskatalógus pedig kifejezetten olyan szekrényeket említ, amelyek több szervert és perifériát védenek. A szekrény kulcsa a fizikai belépést ellenőrző eszközök nyilvántartásába tartozik, elvesztés vagy jogosultságvesztés esetén a zárat cserélni kell. A szekrénybe kerül a rendezőpanel és a kapcsoló is, mert jelentős osztályban a rendszerelosztókhoz és az átviteli vezetékekhez való fizikai hozzáférést külön szabályozni kell.

² 7/2024. (VI. 24.) MK rendelet 2. melléklet 13.2. pont, 13.2.1.8. alpont (A, J, M)

A helyiség belépési rendjét a fizikai védelmi szabályzatban kell rögzíteni, a belépésre jogosultak listáját pedig a szervereket tartalmazó helyiségre is értelmezni kell. Ha a helyiség irodaként működik, a takarító, a karbantartó és a látogató kíséret nélkül nem tartózkodhat ott, vagy a szekrény zártsága önmagában biztosítja, hogy jogosulatlan személy a rendszerelemekhez ne férjen hozzá. Ezt a döntést a kockázatelemzésben indokolni kell. A környezeti feltételek felügyeletét egy hálózatra kötött, riasztást küldő hőmérséklet- és páratartalom-érzékelő megoldja. Az irodai légkondicionálás munkaidőn kívüli kikapcsolása a leggyakoribb hibaforrás, ezért a szekrény hűtéséről külön kell rendelkezni.

A tűz- és vízvédelem a létesítmény meglévő rendszereire építhető. A független energiaforrással rendelkező tűzérzékelést az épület tűzjelző rendszere vagy egy akkumulátoros, a szekrény közelében elhelyezett füstérzékelő biztosítja. A vízkár elleni védelem a főelzáró szelepek ismeretét és hozzáférhetőségét kívánja meg, valamint azt, hogy a szekrény ne kerüljön vizes helyiség, vízvezeték vagy beázásra hajlamos tető alá. A jelentős osztály többletkövetelményeit, a szünetmentes áramellátást és a vészkapcsolást, a szekrénybe épített UPS és egy jelölt, jogosulatlanul nem működtethető áramtalanító kapcsoló teljesíti.

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 A vizsgálat kiindulópontjai

Az állásfoglalás abból indul ki, hogy a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja alá tartozik, és kiberbiztonsági felügyeletét a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) látja el.³ A válasz lényege a többi szervezettípusra is irányadó, a közzsférába tartozó szervezetek eltéréseit külön pont foglalja össze.

A törvény a védelmet nem szűkíti a szoftverre és az adatra. A védelem tárgya az adatok kezelésére használt eszközök összessége, ideértve a környezeti infrastruktúrát, a hardvert, a hálózatot és az adathordozókat.⁴ A szervezet vezetője határozza meg a kockázatokkal arányos védelmi intézkedéseket,⁵ és az EIR biztonsági osztálya alapján valósítja meg az informatikáért felelős miniszter rendeletében előírt intézkedéseket.⁶ Ezeket a 7/2024. (VI. 24.) MK rendelet 2. mellékletének 12. követelménycsoportja (Fizikai és környezeti védelem) tartalmazza. A rendelet emellett kimondja, hogy a szervezetre a szabályzataiban meghatározott adminisztratív, logikai és fizikai védelmi intézkedések irányadók.⁷

4.2 A szerverszoba nem jogszabályi fogalom

A Kiberbiztonsági tv. és a 7/2024. (VI. 24.) MK rendelet egyetlen olyan rendelkezést sem tartalmaz, amely szerverszoba kialakítását írná elő. A rendelet a fizikai védelem tárgyát két kifejezéssel jelöli. Az egyik az „EIR-nek helyet adó létesítmény”, vagyis az épület vagy

³ 2024. évi LXIX. tv. 23. § (1) bekezdés b) pont

⁴ 2024. évi LXIX. tv. 5. § (2) bekezdés a) pont

⁵ 2024. évi LXIX. tv. 6. § (3) bekezdés 6. pont

⁶ 2024. évi LXIX. tv. 10. § (4) bekezdés

⁷ 7/2024. (VI. 24.) MK rendelet 2. § (2) bekezdés

telephely, ahol a rendszer működik. A másik a „rendszerlelemet tartalmazó helyiség”, amely a létesítményen belüli kisebb tér. A szerverszoba kifejezés egyetlen helyen, példaként szerepel.

12.37. A szervezet:

12.37.1. Meghatározott biztonságos szinten tartja a hőmérsékletet, a páratartalmat, a légnyomást és a sugárzást az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (például: adatközpont, szerver szoba, központi gépterem).

12.37.2. Felügyeli a környezeti szabályozási szinteket a szervezet által meghatározott gyakorisággal [7/2024. (VI. 24.) MK rendelet 2. melléklet

12.37. pont] (A, J, M)

A rendelkezés nem azt mondja, hogy a szervezetnek szerverszobát kell fenntartania, hanem azt, hogy ahol az informatikai erőforrások koncentráltan vannak, ott a környezeti feltételeket kézben kell tartani. A követelmény forrása a NIST SP 800-53 katalógus PE-14 kontrollja, amelynek magyarázata szerint a környezeti szabályozás elsősorban a rendszererőforrásokat koncentráltan tartalmazó létesítményekre, például adatközpontokra és szerverszobákra vonatkozik.⁸ Ha a Szervezet a szervereit egy irodában helyezi el, az az iroda válik ilyen helyiséggé, a követelmény pedig oda vándorol.

Ugyanezt az értelmezést erősíti a rendelet 1. melléklete, amely szerint a létesítményekkel kapcsolatos védelmi intézkedések csak azokra a létesítményekre alkalmazandók, amelyek közvetlenül védelmet vagy biztonsági támogatást nyújtanak az EIR-nek, vagy kapcsolatosak azzal.⁹ A fizikai védelmi intézkedések tehát nem a szervezet minden helyiségére vonatkoznak, hanem azokra, amelyek az EIR-t befogadják vagy védik. A szervezet maga dönti el, melyik helyiség ez, a döntés következményeit azonban viselnie kell. Minél kisebb és minél inkább erre a célra szolgál ez a helyiség, annál kevesebb intézkedést kell rá alkalmazni, ami önmagában a különálló szerverszoba mellett szól.

4.3 Ami minden biztonsági osztályban kötelező

Az alap biztonsági osztály követelményei határozzák meg azt a minimumot, amelyet bármely elhelyezésnek teljesítenie kell. A belépés szabályozása a létesítményre vonatkozik.

12.2. A szervezet

12.2.1. Összeállítja, jóváhagyja és kezeli az EIR-eknek helyet adó létesítményekbe belépésre jogosultak listáját.

[...]

12.2.3. A szervezeti előírások szerinti gyakorisággal rendszeresen felülvizsgálja a belépésre jogosult személyek listáját.

⁸ NIST SP 800-53 Rev. 5, PE-14 Environmental Controls, Discussion („The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centers, mainframe computer rooms, and server rooms).”)

⁹ 7/2024. (VI. 24.) MK rendelet 1. melléklet 3.2.2.1. pont

12.2.4. Eltávolítja a belépésre jogosult személyek listájáról azokat, akik már nem jogosultak a belépésre. [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.2. pont] (A, J, M)

A belépés ellenőrzése is minden osztályban kötelező, és ez az a pont, amely a helyiségek kérdését először felveti.

12.6. A szervezet:

12.6.1. Kizárólag a szervezet által meghatározott be- és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést. [...]

12.6.2. Naplózza a fizikai be- illetve kilépéseket.

12.6.3. Ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket.

12.6.5. Megóvjaa a kulcsokat, hozzáférési kódokat és az egyéb fizikai hozzáférést biztosító eszközöket.

12.6.6. Nyilvántartást vezet a fizikai belépést ellenőrző eszközökről, és meghatározott gyakorisággal frissíti azt.

12.6.7. Meghatározott rendszerességgel megváltoztatja a hozzáférési kódokat és kulcsokat, illetve ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az azokkal rendelkező személy elveszíti a belépési jogosultságát. [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.6. pont] (A, J, M)

A 12.6.3. pont a létesítményen belüli helyiségek ellenőrzés alatt tartását kívánja meg, de nem mondja ki, hogy a rendszerelemeknek külön helyiségben kell lenniük. Alap osztályban a rendelet megelégszik azzal, hogy a szervezet tudja, ki hova léphet be, ezt naplózza, a látogatót kíséri, a kulcsokat kezeli. Mindez egy zárható rackszekrénnel felszerelt irodában is teljesíthető, ha a szekrény kulcsa a nyilvántartott kulcsok közé tartozik, és az irodába belépők köre a belépésre jogosultak listájával egyezik. Különálló szerverszobában ugyanez a helyiség zárásával és egy rövid belépési listával teljesül, ezért javaslatunk alap osztályban is a külön helyiség.

Ugyancsak minden osztályban kötelező a fizikai védelmi szabályzat és eljárásrend kiadása,¹⁰ a fizikai hozzáférések felügyelete és a naplók átvizsgálása,¹¹ a látogatói belépések nyilvántartása,¹² a vészvilágítás,¹³ a rendszerelemek be- és kiszállításának engedélyezése és nyilvántartása,¹⁴ valamint a csővezetékek rongálódásából eredő vízkár elleni védelem.¹⁵ Ez utóbbihoz a főelzáró szelepeknek hozzáférhetőnek, működőképesnek és a nélkülözhetetlen szerepköröket betöltő személyek számára ismertnek kell lenniük. A tűzvédelem alapkövetelménye is minden osztályban azonos.

¹⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.1. pont (A, J, M)

¹¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.17. pont (A, J, M)

¹² 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.22. pont (A, J, M)

¹³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.31. pont (A, J, M)

¹⁴ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.42. pont (A, J, M)

¹⁵ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.40. pont (A, J, M)

12.33. A szervezet független energiaforrással rendelkező tűzérzékelő, illetve tűzoltó rendszereket tart fenn és alkalmaz az EIR-ek védelme érdekében. [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.33. pont] (A, J, M)

Irodában ezek is teljesíthetők, de csak tudatos gondoskodással. A rendelet 3. mellékletének fenyegetéskatalógusa a tüzet, a vizet, a kedvezőtlen környezeti feltételeket, az áramellátás megszakadását, az eszközök eltulajdonítását és a helyiségekbe történő engedély nélküli behatolást önálló fenyegetésként sorolja fel.¹⁶ A kockázatelemzésnek ezért ezekre az irodai elhelyezés esetén is ki kell térnie.

4.4 A jelentős és a magas osztály többletkövetelményei

Jelentős osztályban a rendelet a létesítményen belüli infrastruktúra védelmét bővíti. Kötelezővé válik a rendszerelosztókhoz és az átviteli vezetékekhez való fizikai hozzáférés szabályozása,¹⁷ a kimeneti eszközök hozzáférés-ellenőrzése,¹⁸ a behatolásjelző és felügyeleti berendezések alkalmazása a fizikai hozzáférési pontokon,¹⁹ az áramellátó berendezések és a kábelezés védelme,²⁰ a vészkapcsolás,²¹ a szünetmentes áramellátás,²² valamint az automatikusan riasztó tűzjelzés.²³ Ezek közül a rendszerelosztók és a kábelezés védelme az, amely irodai környezetben a legnehezebben biztosítható, mert a rendezőpanel, a kapcsoló és a kábelnyomvonal jellemzően szabadon hozzáférhető. A zárt rackszekrény ezt csak a szekrényen belül oldja meg, ezért jelentős osztályban a különálló szerverszoba javaslata még erősebb, mint alap osztályban.

Magas osztályban a rendelet a helyiség szintjére lép. Három, csak ebben az osztályban kötelező követelmény együttesen teszi szükségessé a külön helyiséget.

12.7. A szervezet a létesítménybe történő fizikai belépés ellenőrzésén túlmenően külön engedélyhez köti a fizikai belépést a szervezet által meghatározott fizikai helyiségekbe, amelyek egy vagy több rendszerelemet tartalmaznak. [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.7. pont] (M)

12.21. A szervezet a létesítménybe történő fizikai belépések ellenőrzésén túl külön figyelmet fordít az EIR egy vagy több elemét tartalmazó helyiségekbe történő fizikai belépésekre. [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.21. pont] (M)

12.44. A szervezet úgy helyezi el az EIR elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti

¹⁶ 7/2024. (VI. 24.) MK rendelet 3. melléklet 1. pont, a táblázat 2., 3., 4., 9., 17. és 45. sora

¹⁷ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.14. pont (J, M)

¹⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.15. pont (J, M)

¹⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.18. pont (J, M)

²⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.24. pont (J, M)

²¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.27. pont (J, M)

²² 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.28. pont (J, M)

²³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 12.34. pont (J, M)

veszélyekből adódó lehetséges kárt, valamint a jogosulatlan hozzáférés lehetőségét. [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.44. pont] (M)

A 12.7. pont a NIST PE-3(1) kontroll megfelelője, amelynek magyarázata szerint a rendszerhez való fizikai hozzáférés ellenőrzése további védelmet ad a létesítmény azon területein, ahol a rendszerelemek koncentrálódnak.²⁴ A külön engedély csak akkor értelmezhető, ha a helyiségbe a létesítménybe belépésre jogosultak nem léphetnek be automatikusan. Egy irodában, ahol a munkatársak dolgoznak, ez nem valósítható meg. A 12.44. pont a jogosulatlan hozzáférés lehetőségének minimalizálását kívánja meg, ami szintén az elkülönített tér mellett szól. Álláspontunk szerint magas osztályban a szervereknek és a központi hálózati eszközöknek külön zárt, a többi helyiségtől eltérő jogosultsággal megközelíthető helyiségben kell lenniük. Hogy ezt a helyiséget szerverszobának, gépteremnek vagy technikai helyiségnek nevezik, közömbös.

4.5 Az irodai elhelyezés és a zárható szekrény

A rendelet a zárható házat opcionális intézkedésként ismeri.

12.10. A szervezet a meghatározott rendszerelemek védelmében zárható fizikai házat vagy egyéb burkolatot alkalmaz a jogosulatlan fizikai hozzáférés megakadályozására. [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.10. pont] (O)

Az opcionális minősítés azt jelenti, hogy a szekrény alkalmazása nem kötelező, nem pedig azt, hogy nem számít. A NIST forráskatalógus a PE-3(4) kontroll magyarázatában rögzíti, hogy a zárható házak mérete az egyetlen hordozható számítógépet védő egységtől a több szervert védő teljes szekrényig terjed.²⁵ Alap és jelentős osztályban ez a szekrény teszi lehetővé, hogy a 12.6.3. pont szerinti ellenőrzés a helyiség helyett a szekrény zártságával valósuljon meg.

Ha a Szervezet valamely követelményt az irodai elhelyezés miatt nem tud a rendelet szövege szerint teljesíteni, a rendelet 1. melléklete két utat kínál. Az egyik az eltérés, amelyet a szervezet dokumentál és indokol, bemutatva, hogy az általa választott intézkedések hogyan biztosítanak egyenértékű biztonsági képességet.²⁶ A másik a helyettesítő védelmi intézkedés, amely az adott biztonsági osztályhoz tartozó intézkedés helyett akkor alkalmazható, ha egyenértékű vagy összemérhető védelmet nyújt a rendszerre valós fenyegetést jelentő veszélyforrások ellen, és a helyettesített intézkedéssel egyenértékű módon biztosítja a külső és belső követelményeknek való megfelelést.²⁷ Mindkét út dokumentálást és a szervezet vezetője vagy a kockázatok felvállalására jogosult személy jóváhagyását kívánja meg.²⁸ Az irodai elhelyezés tehát nem tilos, de nem is magától értetődő. Az auditor nem azt kérdezi, van-e szerverszoba, hanem azt, hogy a rendszerbiztonsági terv szerinti helyiségre a 12. követelménycsoport előírásai hogyan

²⁴ NIST SP 800-53 Rev. 5, PE-3(1) System Access, Discussion („Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.”)

²⁵ NIST SP 800-53 Rev. 5, PE-3(4) Lockable Casings, Discussion („Such casings come in a variety of sizes, from units that protect a single notebook computer to full cabinets that can protect multiple servers, computers, and peripherals.”)

²⁶ 7/2024. (VI. 24.) MK rendelet 1. melléklet 3.1.2. pont

²⁷ 7/2024. (VI. 24.) MK rendelet 1. melléklet 4.1. pont

²⁸ 7/2024. (VI. 24.) MK rendelet 1. melléklet 3.1.3. és 4.2.4. pont

teljesülnek, és hol ennek a bizonyítéka. Különálló szerverszobánál ez a bizonyíték jórészt magából a helyiségből adódik, irodai elhelyezésnél viszont minden pontot külön kell igazolni. Ezért javasoljuk a szerverszobát minden biztonsági osztályban.

4.6 A felhőhasználat hatása

A részben helyi rendszereket üzemeltető szervezetnek a fentiek alapján nem kell mindenképpen szerverszoba, a különálló helyiséget azonban a helyben maradó rendszerek osztályától függetlenül javasoljuk. A szükséges védelmi szintet a biztonsági osztály határozza meg, nem az, hogy a szervezet használ-e felhőt. A felhő azonban két ponton befolyásolja az elemzést. Az egyik a rendelkezési jog terjedelme.

(3) Ha a szervezet rendelkezési joga az elektronikus információs rendszernek csak egyes elemeire vagy funkcióira terjed ki, a 2. mellékletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni. [7/2024. (VI. 24.) MK rendelet 2. § (3) bekezdés]

A felhőszolgáltató adatközpontjában működő rendszerelemek fizikai védelmét a szervezet nem maga valósítja meg. A törvény szerint közreműködő igénybevétele esetén a szervezet vezetője gondoskodik arról, hogy a szükséges kiberbiztonsági követelmények szerződéses kötelekmént teljesüljenek,²⁹ a feladatokért való felelőssége pedig ebben az esetben is fennmarad.³⁰ A fizikai védelmi követelmények tehát a szolgáltatói szerződésben, a szolgáltató tanúsítványában és auditjelentéseiben jelennek meg, nem a szervezet saját helyiségeiben.

A másik az, ami a telephelyen marad. Az elektronikus információs rendszer fogalma minden olyan eszközt és összekapcsolt eszközcsoporthoz magában foglal, amely digitális adatok automatizált kezelését végzi,³¹ és a szervezet rendelkezésében lévő rendszer a szervezet rendszerének minősül.³² A tűzfal, a kapcsolók, a hozzáférési pontok, a munkaállomások és a nyomtatók a kizárólag felhőt használó szervezetnél is rendszerelemek, a telephely pedig ezeknek helyet adó létesítmény. A 12. követelménycsoport ezekre változatlanul vonatkozik, a rendelet 1. melléklete szerint azonban csak annyiban, amennyiben a működtetési környezet ezt szükségessé teszi.³³ Egy kizárólag felhőt használó szervezetnek ezért nem kell szerverszoba, de a hálózati eszközöket zárható szekrényben kell tartania, a kulcsokat és a belépésre jogosultak listáját pedig vezetnie kell.

5. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS 2 irányelv)
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)

²⁹ 2024. évi LXIX. tv. 6. § (5) bekezdés d) pont

³⁰ 2024. évi LXIX. tv. 6. § (6) bekezdés

³¹ 2024. évi LXIX. tv. 4. § 24. pont b) alpont

³² 2024. évi LXIX. tv. 6. § (1) bekezdés

³³ 7/2024. (VI. 24.) MK rendelet 1. melléklet 3.2.1.1. pont

- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 418/2024. (XII. 23.) Korm. rendelet a Kiberbiztonsági tv. végrehajtásáról
- NBSZ NKI, EiR útmutató, Fizikai és környezeti védelem (ver. 1.0, 2024)
- NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations (PE-3, PE-14, PE-18)