Milyen kiberbiztonsági előírások vonatkoznak HO-ban dolgozó munkavállalókra?

VFP2 KiberVéd - NIS2 Audit felkészítés iránymutatás 2026/8

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.14.	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

A Szabályozott Tevékenységek Felügyeleti Hatósága által véleményezett dokumentum

1. ÖSSZEFOGLALÁS

Jelen dokumentum a távmunka (home office, a továbbiakban: HO) keretében végzett munkavégzés kiberbiztonsági kockázatait és az azokra vonatkozó, a NIS2 irányelv hazai implementációjából (különösen a 2024. évi LXIX. törvény és a 7/2024. (VI. 24.) MK rendelet) eredő kötelező védelmi intézkedéseket vizsgálja.

A legfontosabb tanulságok:

- A kiberbiztonsági szabályozás teljes mértékben kiterjed a home office környezetre; az nem egy védett zóna, hanem egy kiemelt kockázati tényező és megnövekedett támadási felület.
- A munkáltató teljeskörűen felelős a HO-ban kezelt vállalati adatok és a HO-ból elért rendszerek (EIR-ek) biztonságáért, függetlenül a fizikai helyszíntől.
- A HO biztonság kulcsa a kockázatalapú megközelítés, amely kötelező technikai (pl. többfaktoros hitelesítés, VPN, eszköztitkosítás, végpontvédelem) és szervezeti (pl. szabályzatok, célzott képzés) intézkedéseket ír elő.
- A munkáltatónak a megfelelőség biztosítása érdekében joga és kötelessége ellenőrizni a vállalati eszközök és a hálózati hozzáférés biztonsági megfelelőségét (pl. MDM/MAM eszközökkel, naplóelemzéssel), de mindezt a munkavállaló magánszférájának tiszteletben tartásával (az Mt. és a GDPR keretei között) kell megtennie.

2. A VIZSGÁLANDÓ KÉRDÉS

A hibrid és távmunka (HO) modellek elterjedésével a szervezetek kiberbiztonsági támadási felülete jelentősen megnövekedett. A munkavállalók az irodai, védett hálózati környezeten kívülről csatlakoznak a vállalati rendszerekhez, gyakran nem megfelelően biztosított otthoni hálózatokról.

Ezzel párhuzamosan a NIS2 irányelv és a hazai implementációja (Kiberbiztonsági tv. 7/2024. MK rendelet) szigorú, kockázatalapú védelmi intézkedéseket és vezetői felelősséget követel meg az Elektronikus Információs Rendszerek (EIR) védelme érdekében.

A kiberbiztonsági auditra való felkészülés során a HO-val kapcsolatban az alábbi kérdéseket érdemes tisztázni:

- Milyen konkrét kiberbiztonsági előírások vonatkoznak a HO-ban dolgozó munkavállalókra?
- Milyen eszközökkel segítheti a munkáltató az előírások betartását a HO környezetben?
- Mi a munkavállaló felelőssége és milyen alapvető elveket kell alkalmaznia a biztonságos munkavégzés érdekében?

3. A HOME OFFICE-BAN DOLGOZÓ MUNKAVÁLLALÓKRA VONATKOZÓ ELŐÍRÁSOK

A kiberbiztonsági követelmények jogszabályi alapját a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) teremti meg, amely előírja a kockázatokkal arányos védelmi intézkedések alkalmazását. A konkrét technikai és adminisztratív kontrollokat a 7/2024. (VI. 24.) MK rendelet (MK rendelet) 2. melléklete tartalmazza.

Az MK rendelet szerint a szervezetnek dokumentálnia kell, hogy kik dolgozhatnak otthonról, és milyen védelmi intézkedések érvényesek rájuk.

> *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;*
> *12.43.3. értékeli a védelmi intézkedések hatékonyságát az alternatív munkavégzési helyeken;*
> *12.43.4. biztosítja a szükséges eszközöket a munkavállalók számára, hogy egy biztonsági esemény bekövetkezése esetén kommunikálni tudjanak az információbiztonságért felelős személyekkel.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 12.43. pont] (A, J, M)*

Ez a gyakorlatban azt jelenti, hogy a munkáltatónak rendelkeznie kell egy jóváhagyott, és a munkavállalókkal megismertetett „Home Office szabályzattal” és a feleknek távmunka-megállapodást kell kötnie, amely rögzíti a biztonsági elvárásokat (pl. ne lásson rá illetéktelen családtag a képernyőre, ne használja más az eszközt).

A Home Office alapja, hogy a munkavállaló távolról, a saját vagy más szervezet internetelérését felhasználva éri el a szervezet belső rendszereit. Erre vonatkozóan szigorú technikai és adminisztratív előírások vannak.

Minden távoli hozzáférési típust (pl. VPN, RDP, felhő alapú elérés) külön engedélyezni kell és dokumentálni.

> *2.100. A szervezet:*
> *2.100.1. Kidolgozza és dokumentálja az engedélyezett távoli hozzáférés minden egyes típusára vonatkozóan a használati korlátozásokat, a konfigurációs vagy csatlakozási követelményeket és az alkalmazási útmutatókat.*
> *2.100.2. Engedélyezési eljárást folytat le a rendszerhez való távoli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 2.100. pont] (A, J, M)*

A távoli munkavégzés során az adatkommunikációnak titkosítottnak kell lennie (pl. VPN használata kötelező), hogy az otthoni internetkapcsolaton keresztül ne lehessen lehallgatni az adatforgalmat. A veszély fokozottabb, ha a munkavállaló nem a saját otthonából, hanem esetleg

egy nyilvános hely (pl. kávézó, étterem, vasút, reptér stb.) internetkapcsolatát használja. Ezekre az esetekre akkor is készülni kell védelmi intézkedésekkel, ha az ilyen internetkapcsolat használata sérti a HO szabályzatot.

> *2.102. A szervezet kriptográfiai mechanizmusokat alkalmaz a távoli hozzáférés biztonságának és sértetlenségének biztosítása érdekében.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 2.102. pont] (-, J, M)*

Biztonsági kockázatot jelent, ha a munkavállaló őrizetlenül hagyja a bejelentkezett eszközt. A rendszernek képesnek kell lennie a kapcsolat bontására inaktivitás esetén.

> *2.106. A szervezet biztosítja a rendszerhez való távoli hozzáférés meghatározott időn belüli szétkapcsolásának vagy letiltásának a lehetőségét.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 2.106. pont]*

A Home Office-ban használt eszközök (amelyek a jogszabály értelmében mobil eszköznek minősülnek, ha elhagyják a szervezet területét) fizikai és logikai védelme kritikus.

Kiemelt követelmény, hogy az eszközökön tárolt adatok titkosítva legyenek (pl. BitLocker, FileVault), így lopás vagy elvesztés esetén az adatok nem hozzáférhetőek.

> *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] (-, J, M)*

Szigorúan szabályozni kell, hogy milyen eszköz csatlakozhat a hálózatra (pl. jogos igény lehet második monitor csatlakoztatása HO környezetben is vagy esetleg nyomtató csatlakoztatása).

> *2.113. A szervezet:*
> *2.113.1. Kialakítja a konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatót az általa ellenőrzött mobil eszközök számára, beleértve azokat az eseteket is, amikor ezek az eszközök a szervezet által ellenőrzött területen kívül helyezkednek el.*
> *2.113.2. Engedélykötelessé teszi a szervezet rendszereihez mobil eszközökkel történő kapcsolódást.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 2.113. pont] (A, J, M)*

A távoli hozzáférés egyik legfontosabb védelmi vonala a többtényezős hitelesítés (Multi-Factor Authentication - MFA). A jogszabály ezt Alap biztonsági osztályban csak privilegizált fiókoknál teszi kötelezővé, Jelentős és Magas magasabb biztonsági osztályokban ez már minden felhasználónál elvárt. A távoli hozzáférés kontrollálása érdekében a MFA minden felhasználó esetén ajánlott (biztonsági osztálytól függetlenül), amihez szükség lehet a munkáltató által biztosított mobiltelefonra is.

> *8.3. A szervezet többtényezős hitelesítést alkalmaz a privilegizált fiókokhoz való hozzáféréshez.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 8.3. pont] (A, J, M)*

> *8.4. A szervezet többtényezős hitelesítést alkalmaz a nem privilegizált fiókokhoz való hozzáféréshez.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 8.4. pont] (J, M)*

A technikai védelem mellett a munkavállaló felelőssége is rögzítésre került. A munkavállalónak nyilatkoznia kell a szabályok megismeréséről.

> *13.3.2. A szervezet az EIR-hez való hozzáférés engedélyezése előtt dokumentált nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az EIR használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 13.3.2. pont] (A, J, M)*

A szervezet korlátozhatja a közösségi média és egyéb nem munkacélú oldalak használatát a szervezet eszközein a kockázatok csökkentése érdekében.

> *13.4. A szervezet a viselkedési szabályaiba a következő korlátozásokat építi be:*
> *13.4.1. a közösségi média, közösségi oldalak és külső oldalak, valamint alkalmazások használatának korlátozása;*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 13.4. pont] (A, J, M)*

Az előírások betartását nem csak a szervezet belső ellenőrzésének, hanem a kétévente kötelező kiberbiztonsági auditnak is vizsgálnia kell. Az audit kiterjed a távoli munkavégzés szabályaira is.

> *(3) A kiberbiztonsági audit kiterjed*
> *[...] f) a szervezet által meghatározott eljárások gyakorlati megvalósulása vizsgálatára.*
> *[1/2025. (I. 31.) SZTFH rendelet 1. § (3) bekezdés f) pont]*

4. MILYEN ESZKÖZÖKKEL ELLENŐRIZHETI A MUNKÁLTATÓ A MEGFELELŐSÉGET?

A munkáltatónak a Kiberbiztonsági tv. alapján joga és kötelessége ellenőrizni a vállalati eszközöket és a hozzáférést a megfelelőség érdekében. Fontos, hogy az ellenőrzés nem a munkavállaló otthoni "kémlelése", hanem a vállalati eszközök biztonsági állapotának (megfelelőségének) automatizált vizsgálata. (Az nem kiberbiztonsági, hanem munkajogi kérdés, hogy a munkáltató milyen munkajogi jogkövetkezményeket alkalmaz a HO-szabályok megsértése esetén – pl. ha azt észleli, hogy a munkavállaló nem az otthonában, hanem más helyen használta az eszközöket).

A szervezet részéről az alábbi jó gyakorlatok alkalmazása javasolt a kockázatok kezelésére:

- **Szabályozás**

- Hozzon létre egyértelmű, írásos Információbiztonsági Szabályzatot (IBSZ) és kapcsolódó eljárásrendeket, amelyek egyértelműen tiltják az IT eszközök magáncélú használatát.
- Ugyanígy javasolt a saját eszköz munkavégzésre történő használatának tiltása is. A munkáltató engedélyezheti, hogy a munkavállaló telepítsen ilyen eszközre az otthoni munkavégzéshez szükséges távoli hozzáférésre szolgáló alkalmazásokat. A munkáltató által biztosított laptop használata lényegesen kevesebb biztonsági és jogi kockázattal jár.
- Javasolt szabályozni a távmunkavégzés kereteit („Home Office szabályzat") és meg kell kötni távmunka végzésre vonatkozó megállapodást a munkavállalókkal, amiben rögzíteni szükséges a specifikus biztonsági elvárásokat, a munkáltató általi ellenőrzés, valamint a munkáltató által biztosított számítástechnikai vagy elektronikus eszköz használata korlátozásának szabályait.

- **Kommunikáció és képzés**
  - Biztosítani kell, hogy minden munkavállaló megismerje és megértse a szabályzatot.
  - Rendszeres biztonságtudatossági képzést kell tartani, amely kifejezetten kitér a magánhasználat tiltásának okaira (pl. kiberbiztonsági kockázatok, adatszivárgás) és az elvárt viselkedésre.
- **Technikai védelmi intézkedések bevezetése**
  - Szoftvertelepítés korlátozása: a szervezet technikailag tiltsa meg, hogy a felhasználók szoftvereket telepíthessenek az eszközökre, és alkalmazzon "alapértelmezett tiltás, kivétel alapú engedélyezés" elvet (allow-listing).
  - A munkáltató által biztosított eszközökön a biztonsági frissítések telepítésének kikényszerítése.
  - Adathordozók és perifériák tiltása esetén a szervezet korlátozza vagy tiltsa meg a nem engedélyezett külső adathordozók (pl. személyes USB-meghajtók) és perifériák csatlakoztatását.
  - Hálózati hozzáférés szűrését érintően a szervezet korlátozza a hozzáférést a munkavégzéshez nem szükséges weboldalakhoz, különösen a személyes levelezőrendszerekhez, közösségi média oldalakhoz és külső felhőtárhelyekhez.
  - Adatmozgás korlátozása esetén a szervezet alkalmazzon technikai megoldásokat (pl. DLP - Data Loss Prevention) a szervezeti adatok magáncélú rendszerekbe (pl. privát e-mail) történő átmásolásának megakadályozására.
  - Eszközfelügyelet elvégzése vállalati mobil eszközök esetén a szervezet alkalmazzon központi felügyeleti rendszert (MDM – Mobile Device Management) a céges biztonsági házirendek kikényszerítésére. A munkavállalók technikai ellenőrzésével kapcsolatos döntés meghozatala és a szabályzat véglegesítése előtt konzultáljon adatvédelmi szakértővel, hogy a szabályozás és az esetleges ellenőrzési pontok megfeleljenek a GDPR és az Mt. előírásainak. Saját tulajdonú mobil eszköz (BYOD) esetén MAM - Mobile Application

Management megoldás ajánlott, mert Ellentétben az MDM-el, ami az egész eszközt kezeli regisztrációval, a MAM csak az app-szintű adatokat és működést szabályozza anélkül, hogy az eszköz teljes hozzáférését megkövetelné.

- **Ellenőrzés és kilépési folyamat**
  - Alkalmazzon naplózást és monitorozást a rendszerszintű, szokatlan tevékenységek észlelése érdekében (pl. nagy mennyiségű adatmozgás), tiszteletben tartva a munkavállalók magánszféráját és az Mt. 11/A. és 196 - 197 §-aiban foglaltakat.
  - Arra az esetre, ha a tiltás ellenére a felhasználó mégis magáncélú tartalmat tárol az eszközön, a kilépő munkavállalókkal kilépéskor írasson alá nyilatkozatot arról, hogy minden (a tiltás ellenére esetlegesen ott lévő) magáncélú tartalmukat mentették és eltávolították a szervezet hardver és szoftver eszközeiről.

5. A MUNKAVÁLLALÓ FELELŐSSÉGE ÉS GYAKORLATI TEENDŐI

A technikai kontrollok mellett elengedhetetlen a munkavállalói tudatosság és az alapvető elveknek, elvárásoknak megfelelő alkalmazása. A munkavállaló felelőssége, hogy betartsa a szabályokat és aktívan hozzájáruljon a biztonsághoz.

- **Fizikai biztonság**
  - A gép azonnali zárolása (pl. Win+L), ha feláll mellőle, még akkor is, ha csak egy másik helyiségbe megy ki.
  - A monitor"váll feletti" (shoulder surfing) olvasásának megakadályozása (pl. családtagok, lakótársak, vendégek által, vagy a közeli ingatlanokból).
  - Az eszköz biztonságos tárolása (pl. nem az ablakban hagyva).
- **Adatkezelés**
  - Szigorúan tilos a szervezeti adatokat magáneszközre (pl. saját USB, privát e-mail, saját Google Drive) másolni.
  - Szigorúan tilos bizalmas adatokat otthoni nyomtatón kinyomtatni.
- **Hálózat**
  - Az otthoni Wi-Fi hálózat minimális védelmének biztosítása (pl. WPA2/WPA3 használata, a router alapértelmezett "admin" jelszavának megváltoztatása).
- **Tudatosság**
  - Bármilyen gyanús jel (lassulás, furcsa felugró ablak, gyanús e-mail) azonnali jelentése az IT Helpdesk / SOC felé.
  - A biztonsági frissítések telepítésének a munkáltató által meghatározott határidőn belüli végrehajtása.

6. HOME OFFICE BIZTONSÁGI KOCKÁZATOK ÉS KOCKÁZAT CSÖKKENTŐ INTÉZKEDÉSEK

Az alábbi táblázat összefoglalja a főbb HO-kockázatokat és az azok kezelésére szolgáló, NIS2-kompatibilis védelmi intézkedéseket.

Tevékenység / Kockázat	**Kockázatcsökkentő intézkedés**	**Elsődlegesen kezelt szervezeti kockázat**
Gyenge vagy ellopott jelszó használata távoli eléréshez	Többfaktoros hitelesítés (MFA) kötelező használata minden távoli eléréshez (VPN, e-mail, felhő). Erős jelszópolitika kikényszerítése.	Hitelesítő adatokkal való visszaélés, jogosulatlan hozzáférés, zsarolóvírus fertőzés.
Vállalati laptop elvesztése, ellopása (fizikai hozzáférés)	Kötelező teljes lemezes titkosítás (FDE - BitLocker/FileVault). Távoli törlés képességének biztosítása (MDM – Mobile Device Management vagy MAM - Mobile Application Management)	Adatszivárgás, bizalmas adatokhoz való fizikai hozzáférés, reputációs kár.
Otthoni, nem biztonságos Wi-Fi használata	Kötelező VPN használata a belső rendszerek eléréséhez. "Split tunneling" tiltása javasolt. Az otthoni hálózat minimális biztonságának (WPA2/3) előírása szabályzatban.	Csomaglehallgatás (Man-in-the-Middle), jogosulatlan hálózati hozzáférés.
Biztonsági frissítések halogatása a HO eszközön	Központi, automatizált és kényszerített frissítéskezelés (patch management). A nem megfelelő ("non-compliant") eszközök automatikus kizárása a hálózatról (NAC).	Ismert sebezhetőségek kihasználása, zsarolóvírus fertőzés, rendszerinstabilitás.
Adathalász támadás HO környezetben (emberi tényező)	Célzott biztonságtudatossági képzés (HO-specifikus kockázatokról). Egyértelmű, gyors incidensbejelentési csatorna biztosítása és megismertetése.	Hitelesítő adatok ellopása, kártevő bejutása, lassú incidensreakció.
Vállalati adatok átmásolása magáneszközre (USB, privát e-mail)	Szigorú szabályzati tiltás. Technikai kontrollok (DLP - Data Loss Prevention) alkalmazása, ahol lehetséges (pl. USB portok tiltása).	Adatszivárgás/adatvédelmi incidens, a vállalati adatok feletti kontroll elvesztése, GDPR megfelelőségi kockázat.

Munkavállaló "saját" (BYOD) eszközének használata	Erősen ellenjavallt. Ha elkerülhetetlen, szigorú szabályozás és technikai kontroll (pl. MDM, MAM, konténerizáció) szükséges, de a cég felelőssége és kockázata megmarad. Előnyben részesítendő a vállalati eszköz biztosítása.	Nem felügyelt eszköz (kártevők, hiányzó frissítések), adatszivárgás, a cég kontrolljának elvesztése, jogi viták (adatvédelem).

7. FORRÁSOK

Jogszabályok

- 2012. évi I. törvény a Munka Törvénykönyvéről (Mt.)
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR)
- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS2 irányelv)
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- A Miniszterelnöki Kabinetirodát vezető miniszter 7/2024. (VI. 24.) MK rendelete 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