

Nem támogatott operációs rendszerek (W7, WXP) NIS2-kompatibilis használata, ha azok cseréje nem lehetséges

VFP2 KiberVéd - NIS2 Audit felkészítés szakértői
állásfoglalás 2026/27

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.24	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A Windows XP és a Windows 7 gyártói támogatása évekkel ezelőtt megszűnt, 2025. október 14. óta pedig a Windows 10 is ebbe a körbe tartozik.¹ A régi rendszerek mégis velünk maradnak: a 30-50 éves gyártósorok vezérlői és a 12-15 éves ultrahangkészülékek gyakran csak ezekkel működnek, a csere pedig műszaki, gazdasági vagy engedélyezési okból nem reális.

Álláspontunk szerint a magyar szabályozás nem tiltja a támogatással már nem rendelkező operációs rendszerek használatát. A védelmi intézkedések katalógusa kifejezetten számol ezzel

¹ A Microsoft tájékoztatása szerint a Windows XP támogatása 2014. április 8-án, a Windows 7 támogatása 2020. január 14-én, a Windows 10 támogatása 2025. október 14-én szűnt meg; a Windows 10-hez időben korlátozott kiterjesztett biztonsági frissítési (ESU) program érhető el, amely csak a kritikus és fontos biztonsági javításokat tartalmazza. A Nemzeti Kiberbiztonsági Intézet 2025. október 16-i közleménye a támogatás megszűnésének kockázataként a kártékony kódot, a zsarolóvírust, az adatszivárgást és a jogi felelősséget nevesíti.

a helyzettel, és a csere mellett elismeri a belső vagy külső erőforrással biztosított alternatív támogatást. A feltétel az, hogy a szervezet a kivételt kockázati döntésként kezelje: szerepeljen a kockázatelemzésben és a rendszerelem-leltárban, a szabályzatok rögzítsék a kereteit, a hiányzó gyártói javításokat pedig dokumentált helyettesítő intézkedések pótolják. Ezek elsősorban hálózati szintű kontrollok: offline üzem, elkülönített szegmens, az eszköz köré épített forgalomszűrés és folyamatos figyelés.

A kivételt a szervezet vezetője hagyja jóvá, és kivezetési tervvel együtt időszakonként felül kell vizsgálni. A fizikai elzárás önmagában nem pótolja a vírusvédelmet, mert a kártékony kód a hálózaton és az adathordozókon érkezik, nem az ajtón.

2. A VIZSGÁLANDÓ KÉRDÉS

Az auditokon visszatérő, az auditorok előtt is ismert kérdés, hogy mit kezdjen a szervezet azokkal a speciális célgépekkel, amelyek gyártói támogatással már nem rendelkező operációs rendszert futtatnak. A gyártósori vezérlő cseréje sokszor a teljes gyártósor cseréjét jelentené. Az orvostechikai eszköz operációs rendszerét pedig a gyártó jóváhagyása nélkül nem lehet lecserélni, mert az eszköz a szoftverével együtt minősített termék.² A jogszabály a támogatott szoftverek használatából indul ki, a kérdés tehát az, hogy mekkora mozgástér marad.

A felmerülő kérdések:

- Tiltja-e a Kiberbiztonsági tv. vagy a 7/2024. (VI. 24.) MK rendelet a nem támogatott operációs rendszerek használatát?
- Milyen dokumentációs és adminisztratív feltételekkel tartható meg egy ilyen rendszer?
- Milyen technikai helyettesítő intézkedések fogadhatók el?
- Mi nem fogadható el kiegészítő kontrollként?

3. VÁLASZ

3.1 Tiltja-e a jogszabály a nem támogatott operációs rendszerek használatát?

Nem tiltja. A Kiberbiztonsági tv. a védelmet nem konkrét technológiához, hanem a kockázatokhoz köti, a védelem költségei a fenyegetések által okozható károk értékével arányosak [2024. évi LXIX. törvény 4. § 99. pont d) alpont], a kockázatokkal arányos védelmi intézkedéseket pedig a szervezet vezetője határozza meg [2024. évi LXIX. törvény 6. § (3) bekezdés 6. pont]. A Rendelet³ hibajavítási követelménye valóban a támogatott szoftver képéből indul ki, hiszen frissítést csak akkor lehet telepíteni, ha a gyártó kiad ilyet:

² Az orvostechikai eszközökről szóló (EU) 2017/745 rendelet I. melléklet 17.2. és 17.4. pontja a szoftvert az eszköz részeként kezeli; az operációs rendszer gyártói jóváhagyás nélküli cseréje ezért az eszköz megfelelőségét érintheti (tartalmi összefoglalás).

³ A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: Rendelet), a 2025. január 2. napjától hatályos állapot. A 2. melléklet követelményeinél az „A”, „J”, „M” jelölés az „alap”, a „jelentős”, illetve a „magas” biztonsági osztályban kötelező követelményt, az „O” az egyik osztályban sem kötelező (opcionális) követelményt jelöli.

18.2.3. A biztonsági szempontból releváns szoftver- és firmware-frissítéseket a frissítések kiadását követő meghatározott időtartamon belül telepíti. [7/2024. (VI. 24.) MK rendelet 2. melléklet 18.2.3. pont; A, J, M]

A katalógus azonban külön rendezi a támogatás megszűnésének esetét, és nem a cserét írja elő egyedüli megoldásként:

16.99. A szervezet: 16.99.1. lecseréli a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól; illetve 16.99.2. a támogatással már nem rendelkező rendszerelemekhez alternatív támogatást biztosít, amelyet belső erőforrásokkal vagy a szervezet által meghatározott külső szolgáltatók bevonásával valósít meg. [7/2024. (VI. 24.) MK rendelet 2. melléklet 16.99. pont; A, J, M]

A jogalkotó tehát már az „alap” osztályban is elismeri a támogatás nélküli rendszerelem megtartását, ha a szervezet alternatív támogatásról gondoskodik. Ez összhangban áll a NIS2 irányelv 21. cikkével, amely a technika állását és a végrehajtás költségeit figyelembe vevő, a kockázatokkal arányos intézkedéseket vár el.⁴ A támogatás nélküli rendszer megtartása tehát nem jogsértés, hanem kezelt kivétel: ha a kockázatelemzés indokolja, a szervezet eltérhet a rendszerre vonatkozó biztonsági követelményektől, illetve helyettesítő védelmi intézkedéseket alkalmazhat (1. melléklet 1.1.3. pont).

3.2 Dokumentációs és adminisztratív feltételek

Kockázatelemzés, az elavult operációs rendszer a törvény 4. § 87. pontja szerinti sérülékenységgé ismert, javítatlan gyengeség. A rendszerszintű kockázatelemzésben (2. melléklet 15.4. pont; A, J, M) ezért nevesíteni kell, a fenyegetésekkel és a maradó kockázat besorolásával együtt. A kivétel nem lehet hallgatólagos, a legalacsonyabb kategóriánál magasabb kockázat felvállalását a szervezet vezetője vagy a kockázatok kezeléséért felelős személy kockázatonként indokolva hagyja jóvá (1. melléklet 5.1.2.2. pont).

Az eltérés dokumentálása, az indokolás tartalmát a Rendelet meghatározza:

3.1.2. A szervezet a vonatkozó szabályozásában dokumentálja és indokolja, hogy a jelen rendeletben foglalt védelmi intézkedésektől eltérő, általa meghatározott intézkedések hogyan biztosítják az elektronikus információs rendszer egyenértékű biztonsági képességeit, kockázatokkal arányos biztonsági követelményszintjét, és azt, hogy miért nem használhatók a jelen rendeletben megjelölt védelmi intézkedések. [7/2024. (VI. 24.) MK rendelet 1. melléklet 3.1.2. pont]

⁴ Az (EU) 2022/2555 irányelv 21. cikk (1) bekezdés és (2) bekezdés e) pont (tartalmi összefoglalás). Ugyanezt a logikát követi az (EU) 2024/2690 bizottsági végrehajtási rendelet melléklete, amely a biztonsági javítások kezelése körében (6.6. pont) számol azzal, hogy egy javítás nem áll rendelkezésre vagy nem alkalmazható, és ilyenkor további intézkedéseket, a fennmaradó kockázat elfogadását és a döntés dokumentálását várja el (tartalmi összefoglalás); a magyar szervezetek többségére közvetlenül nem alkalmazandó, értelmezési segédletként azonban irányadó.

A helyettesítő intézkedés csak akkor alkalmazható, ha a katalógusban nincs az adott körülmények között eredményesen alkalmazható intézkedés, a szervezet a helyettesítés kockázatát felméri és elfogadja, az egyenértékűséget bemutatja, a döntést pedig a vezető vagy a kockázatok felvállalására jogosult személy jóváhagyja (1. melléklet 4.2. pont). A dokumentum helye a rendszerbiztonsági terv (1. melléklet 1.1.3. pont); a rendszer további használatáról a vezető át nem ruházható feladatkörében, jegyzőkönyvben dönt (1. melléklet 1.1.6. pont). A Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) és f) pontja szerinti szervezeteknél (közigazgatási ágazat, többségi állami befolyás alatt álló gazdálkodó szervezetek) ennél több kell: a helyettesítő intézkedéseket a nemzeti kiberbiztonsági hatóságnak is be kell jelenteni [418/2024. (XII. 23.) Korm. rendelet 8. § (2) bekezdés b) pont], a továbbhasználatról hozott vezetői döntést pedig a hatóság hagyja jóvá, és meg is tilthatja [418/2024. (XII. 23.) Korm. rendelet 14. § (1) és (3) bekezdés].

Rendszerelem-leltár, a régi gépeket a rajtuk futó operációs rendszer pontos verziójával együtt nyilván kell tartani, mert a leltárnak a rendszer minden elemét pontosan kell tükröznie (2. melléklet 6.36.1. pont; A, J, M). A leltár a jóváhagyott eltéréseket is mutathatja (6.41. pont; O), így az auditor egy helyen látja a kivételeket.

Belső szabályozás, az információbiztonsági szabályzat [2024. évi LXIX. törvény 6. § (3) bekezdés 7. pont] rögzíti a kivételkezelés rendjét, ki kérheti, ki hagyja jóvá, meddig érvényes, milyen kötelező kontrollokkal jár. Új beszerzésnél a szerződésben elő kell írni a biztonsági osztályhoz tartozó védelmi intézkedéseket (2. melléklet 16.7.4. pont; A, J, M), tehát támogatott platformot kell megkövetelni, a támogatás időtartamának kikötésével. A meglévő, nem cserélhető eszközöknél a szabályzat mondja ki, milyen helyettesítő intézkedések nélkül nem üzemelhetnek.

Belső támogatás, a 16.99.2. pont szerinti alternatív támogatás működő képesség: a szervezet ismeri a rendszer sérülékenységeit, figyeli az ezekre épülő támadásokat, mentési képpel és helyreállítási eljárással rendelkezik. Külső szolgáltatónál a kiberbiztonsági követelményeket szerződéses kötelemként kell rögzíteni [2024. évi LXIX. törvény 6. § (5) bekezdés d) pont]. A kivételhez kivezetési terv is tartozik (1. melléklet 1.1.7.4. pont).

3.3 Technikai helyettesítő intézkedések

A régi eszközön a szokásos védelem gyakran nem valósítható meg, nincs támogatott vírusvédelem, a titkosítási protokollok elavultak, a naplózás korlátozott. A Rendelet ezt elviseli, mert a kártékony kód elleni védelmet a rendszer határaitra helyezi:

18.8.1. Kártékony kódok elleni védelmi mechanizmusokat alkalmaz a rendszer belépési és kilépési pontjain, hogy felderítse és megfelelő módon eltávolítsa a kártékony kódokat. [7/2024. (VI. 24.) MK rendelet 2. melléklet 18.8.1. pont; A, J, M]

Ha a régi gép belépési és kilépési pontjai egy szűk, ellenőrzött hálózati határra szűkülnek, a védelem ott valósul meg, ahol az eszköz maga erre képtelen. Az 1. melléklet erre eljárást is ad:

3.2.7. Az elektronikus információs rendszer dokumentáltan elkülönített, informatikai biztonsági szempontból önállóan értékelhető elemei

tekintetében a védelmi intézkedések a szervezet által elfogadott kockázatmenedzsment eljárásrendben rögzített vizsgálatot követően, külön-külön egyedi eltérésekkel is alkalmazhatóak, ha az elkülönített elemek közötti határvédelemről gondoskodtak. A határvédelem megfelelőségét, valamint az egyedi eltérések okát és mértékét dokumentálni és meghatározott gyakorisággal felülvizsgálni szükséges.
[7/2024. (VI. 24.) MK rendelet 1. melléklet 3.2.7. pont]

Az Offline működés, a legbiztonságosabb megoldás, ha az eszköz egyáltalán nem kapcsolódik hálózatra. Az adatmozgatás és a mentés ilyenkor fizikai adathordozón történik, amelynek használatát a szervezet korlátozza (2. melléklet 11.14.1. pont; A, J, M), a külső forrásból származó fájlokat pedig ellenőrzi (18.8.3.1. pont; A, J, M). A gyakorlatban ez vírusellenőrző „zsilip” munkaállomást és címkézett, azonosítható tulajdonosú adathordozókat jelent.

Hálózati szegmentáció. Ha a gépnek hálózaton kell lennie, elkülönített szegmensbe kerül, amely csak menedzselt interfészen érintkezik a többi hálózattal (2. melléklet 17.17. pont; A, J, M). A „jelentős” és a „magas” osztályban a határon az alapértelmezett tiltás kötelező (17.20. pont; J, M), a kivételeket üzleti indokkal és időtartammal kell dokumentálni és rendszeresen felülvizsgálni (17.19.4. és 17.19.5. pont; J, M). Internet-, levelezés- és böngészőhozzáférés a szegmensből nem engedélyezhető.

A Mikroszegmentáció, a közvetlenül a gép köré épített tűzfal vagy hosztalapú határvédelem (17.26. pont; O) tovább szűkíti a forgalmat: csak a nevesített partnerrendszerek, csak a szükséges protokollok és portok, és ahol a folyamat engedi, csak meghatározott típusú állományok (például .doc vagy .xls dokumentumok) mehetnek át. A tiltott portok, protokollok és szolgáltatások meghatározása egyébként is alapkövetelmény (6.26.2. pont; A, J, M).

Kiegészítő intézkedések az eszközön. Ahol az operációs rendszer engedi, az alkalmazás-engedélyezőlista (6.31. pont; J, M) erős kompenzáló kontroll, mert az ismeretlen kód futását javítatlan sérülékenységgel is megakadályozza. Ehhez járul a szegmens és a gép figyelése (18.13. pont; A, J, M), a rendszeres, kiber-fizikai rendszernél elsősorban passzív sérülékenységgellenőrzés (15.9. pont; A, J, M),⁵ a rendszergazdai jogosultságok elvétele és a helyreállítható rendszerkép.⁶

3.4 Mi nem fogadható el?

A fizikai védelem önmagában nem helyettesíti a vírusvédelmet. A helyettesítő intézkedés fogalma ugyanis a valós fenyegetéshez kötött:

4.1. A helyettesítő védelmi intézkedés alkalmazása olyan eljárás, amelyet a szervezet az adott biztonsági osztályhoz tartozó védelmi intézkedés helyett kíván alkalmazni, és egyenértékű vagy összemérhető védelmet

⁵ A 418/2024. (XII. 23.) Korm. rendelet 2. § 14. pontja a kiber-fizikai rendszerek biztonsági vizsgálatát elsősorban passzív technikákkal, a rendszer működésének zavarása nélkül végzett vizsgálatként határozza meg; aktív szkennerek régi vezérlőn üzemzavart okozhat.

⁶ Ugyanezt a logikát követi az ISO/IEC 27001:2022 szabvány A.8.8. (technikai sérülékenységek kezelése), A.8.22. (hálózatok elkülönítése) és A.8.7. (kártékony kód elleni védelem) kontrollja.

nyújt az adott elektronikus információs rendszerre valós fenyegetést jelentő veszélyforrások ellen (...) [7/2024. (VI. 24.) MK rendelet 1. melléklet 4.1. pont]

A szerverterembe zárt gép a jogosulatlan fizikai hozzáférés ellen véd, a kártékony kód azonban a hálózaton vagy az adathordozón érkezik. A zár tehát más fenyegetésre ad választ, mint amit a vírusvédelem és a hibajavítás kezel, ezért nem összemérhető védelem. Ugyanígy nem fogadható el a sehol nem rögzített vagy lejárat nélküli „örökös” kivétel, és az a gyakorlat sem, amikor a régi gép a felhasználói hálózaton marad, és csak a vírusvédelem hiányát fogadják el kockázatként.

Az arányos kiberbiztonsági intézkedések bevezetésének elmulasztása önálló bírságtényállás [418/2024. (XII. 23.) Korm. rendelet 2. melléklet 7. sor], a szervezet vezetője pedig 15 millió forintig terjedő bírsággal sújtható [418/2024. (XII. 23.) Korm. rendelet 42. § (4) bekezdés].⁷ A dokumentált, jóváhagyott és helyettesítő intézkedésekkel kísért kivétel ezzel szemben azt bizonyítja, hogy a szervezet a kockázatot ismeri és kezeli. Betegadatokat kezelő eszközön ugyanazt az általános adatvédelmi rendelet 32. cikke is megköveteli.⁸

4. ELLENŐRZŐLISTA A KIVÉTEL KEZELÉSÉHEZ

1. Az eszköz és operációs rendszere szerepel a rendszerelem-leltárban, verzióval és felelőssel.
2. A kockázatelemzés nevesíti a sérülékenységet és a maradó kockázatot; a felvállalást a vezető indokolással jóváhagyta.
3. A rendszerbiztonsági terv tartalmazza az eltérés indokolását és a helyettesítő intézkedéseket; a)-c) és f) pont szerinti szervezetnél ezt a hatóságnak is bejelentették.
4. Az eszköz offline vagy elkülönített szegmensben üzemel, alapértelmezett tiltással, szabályozott adathordozó-használattal és működő figyeléssel.
5. Van alternatív támogatás, mentés, helyreállítási eljárás és határidős kivezetési terv; a kivételt legalább a biztonsági osztályba sorolás kétévenkénti felülvizsgálatakor újraértékelik [2024. évi LXIX. törvény 10. § (7) bekezdés].

5. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)

⁷ A Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezetekkel szemben a Szabályozott Tevékenységek Felügyeleti Hatósága a 418/2024. (XII. 23.) Korm. rendelet 3. melléklete szerint jár el [418/2024. (XII. 23.) Korm. rendelet 42. § (1) bekezdés b) pont]; ennek 6. sora a Kiberbiztonsági tv. 6. § (2) bekezdése szerinti kockázatmenedzsment-kötelezettség nem teljesítését bírságolja.

⁸ Az (EU) 2016/679 rendelet 32. cikk (1) bekezdése a tudomány és technológia állása, a megvalósítás költségei és a kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket ír elő (tartalmi összefoglalás). A nem támogatott rendszer kompromittálódása adatvédelmi incidens is lehet, amelyet a Nemzeti Adatvédelmi és Információszabadság Hatóságnak külön be kell jelenteni.

- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről (Rendelet)
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- (EU) 2022/2555 irányelv (NIS2) 21. cikk; (EU) 2024/2690 bizottsági végrehajtási rendelet; (EU) 2017/745 rendelet I. melléklet 17. pont; (EU) 2016/679 rendelet 32. cikk
- Nemzeti Kiberbiztonsági Intézet: A Windows 10 támogatásának megszűnésével járó kiberbiztonsági kockázatok (2025. október 16.)